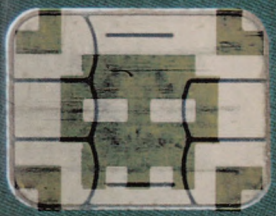


NEMATOMA RINKA

4096 7100 024

4096

GOOD THRU 11/13

ELEKTRONINIAI NUSIKALTIMAI IR JŪS

MISHA GLENNY

baltos lankos

MISHA GLENNY

Nematoma rinka

ELEKTRONINIAI NUSIKALTIMAI IR JŪS

Iš anglų kalbos vertė
MARIJA DALIA TRUČINSKIENĖ

baltos lankos

UDK 343.9:004
Gl-86

Versta iš:
Misha Glenny,
DarkMarket: CyberThieves, CyberCops and You,
Random House, London, 2011

Redaktorė
Dalia Kižlienė

Dailininkas
Zigmantas Butautis

Maketuotojas
Audris Šimakauskas

Šį leidinį draudžiama atgaminti bet kokia forma ar būdu, viešai skelbti, taip pat padaryti viešai prieinamą kompiuterių tinklais (internete), išleisti ir versti, platinti jo originalą ar kopijas: parduoti, nuomoti, teikti panaudai ar kitaip perduoti nuosavybėn.

Draudžiama šį kūrinį, esantį bibliotekose, mokymo įstaigose, muziejuose arba archyvuose, mokslinių tyrimų ar asmeninių studijų tikslais atgaminti, viešai skelbti ar padaryti visiems prieinamą kompiuterių tinklais tam skirtuose terminaluose tų įstaigų patalpose.

ISSN 1822-9247
ISBN 978-9955-23-620-7

© Misha Glenny, 2011
© Marija Dalia Tručinskienė, vertimas į lietuvių kalbą, 2012
© Baltų lankų leidyba, 2012

Skiriama Miljanui, Alexandrai ir Callumui

Turinys

Prologas 9

PIRMA KNYGA

I dalis
1. Skambina inspektorius 27
2. „Miranda“ praneša apie puikų naują pasaulį 35
3. Misteris Haidas iš Lagoso 46

II dalis
4. Odesos failai 57
5. Karderių planeta 65
6. Šeimos afera 67
7. Smauglys prisiraugtas 79
8. Scenarijaus perrašymas 88

III dalis
9. Tigras, tigras 95
10. Žaidimų teorija 100
11. Kelio atgal nėra 104
12. Kelionė į Indiją 111
13. Šešėlinė šalis 115

IV dalis
14. Ledo Žmogus ateina 125
15. Karderių rinka 131
16. Tamsioji rinka 136
17. Biuras 142
18. Įtarūs protai 152
19. Donnie Brasco 157
20. Klastingas planas 166

V dalis
21. Drono palikimas 173
22. Susimovei, vyruti 180
23. Kvadratinė matrica 184
24. Prancūziška jungtis 188
25. Nematomas žmogus 194

Tarpinis epizodas
Man nežinoma nežinia kur esanti šalis 201

ANTRA KNYGA

I dalis
26. Bilalas Pitsburge 229
27. Svarbiausias portalas 240

II dalis
28. *Ciao*, Cha0 247
29. Švelniai švelniai 253

III dalis
30. Merto Ortaço fantazijų pasaulis 263
31. Dviejų ponų tarnas 272
32. Turkiški malonumai 278
33. Sugrįžimas į pragarą 284
34. Turko medžioklė 290
35. Tamsiosios rinkos žlugimas 295

IV dalis
36. Dvigubas pavojus 297
37. Zoro nuplėšta kauke 302
38. Kas tu toks? 309
39. Kelyje į niekur 310
40. Vidurdienio ekspresas 316

Epilogas 321
Pastabos apie duomenų šaltinius 336
Padėkos 338

Prologas

crime@21stcentury.com

Nenuilstamose žmonijos lenktynėse dėl patogumų ir augant ekonomikai per labai trumpą laiką mes pasiekėme pavojingą priklausomybės nuo tinklinių sistemų lygį: trumpiau nei per du dešimtmečius milžiniškos vadinamosios ypatingos svarbos nacionalinės infrastruktūros (CNI, pagal technokratus) dalys daugelyje šalių dabar yra valdomos kas kartą sudėtingesnėmis kompiuterinėmis sistemomis.

Kompiuteriai reguliuoja daugelį mūsų gyvenimo sričių, nes nuo jų priklauso mūsų bendravimas, mūsų transporto priemonės, mūsų santykiai su komercinėmis ir valdžios struktūromis, mūsų darbas, laisvalaikis ir visa kita. Pastaraisiais metais aš dalyvavau keliuose kibernetinių nusikaltimų teisminiuose procesuose, viename iš jų Britanijos karališkoji prokuratūros tarnyba pareikalavo įvesti vadinamąsias nusikaltimo prevencijos orderio sankcijas programišiui (angl. *hacker*), kurios įsigaliotų, paleidus jį iš kalėjimo. Šiuo orderiu jam būtų uždrausta naudotis internetu, išskyrus vieną valandą per savaitę, prižiūrint policijos pareigūnui. „Iki tol, kol mano klientui pasibaigs bausmės laikas, – nagrinėjant bylą pareiškė atsakovo advokatas, – vargu ar bus likusi bent viena žmonijos veiklos sritis, galinti išsiversti be kokio nors interneto tarpininkavimo. Kaip, jūsų manymu, mano klientas sugebėtų gyventi normalų gyvenimą tokiomis aplinkybėmis?“ – retoriškai paklausė jis.

Iš tiesų – kaip? Tie, kuriems yra tekę palikti savo mobilųjį telefoną namie nors kelioms valandoms, paprastai smarkiai susierzina ir patiria praradimo pojūtį, panašų į tą, kurį jaučia žmonės, staiga nusprendę įveikti priklausomybę nuo alkoholio ar narkotikų. Įdomu tai, kad, nenaudojant prietaiso tris dienas, šį žlugdantį nerimo jausmą dažnai pakeičia užplūdęs išsilaisvinimo pojūtis, nes žmogus tarsi sugrįžta į dar tokį netolimą pasaulį, kuriame neturėjome mobiliųjų telefonų ir mums jų nereikėjo, atitinkamai tvarkėme savo gyvenimą be jų.

Šiais laikais daugumai žmonių atrodo, kad jie nebegali gyventi be šių mažyčių nešiojamųjų kompiuterių.

Galbūt geriausiai galima palyginti kompiuterį su automobiliu. Kai nuo praeito amžiaus penktojo dešimtmečio tapo įprasta turėti automobilį kiekvienoje šeimoje, tik mažuma vairuotojų iš tiesų suprato, kas vyksta po variklio dangčiu. Vis dėlto buvo gana daug tokių, kurie mokėjo pataisyti savo automobilį, kad ir kokia būtų jo gedimo priežastis, dar daugiau buvo tokių, kurie sugebėjo sutvarkyti karbiuratorių, kad galėtų lėtai parsigauti iki namų, o dauguma bent jau mokėjo pasikeisti nuleistą padangą.

Šiais laikais, jei problema yra tik nuleista padanga, jūs tikriausiai sugebėsite pasiekti savo kelionės tikslą. Bet vis daugiau gedimų yra susiję su kompiuterio, įmontuoto valdymo bloke – juodo plastiko korpuse, paprastai esančiame už variklio, – gedimais. Jei tai valdymo bloko problema, jūs niekaip neužvesite automobilio, net jei esate patyręs tankų mechanikas. Jei jums pasiseks, inžinierius kompiuterių specialistas sugebės jį sutaisyti. Bet daugeliu atvejų teks pakeisti visą bloką.

Kompiuterinės sistemos daug sudėtingesnės ir jautresnės nei vidaus degimo varikliai, taigi tik maža saujelė žmonių gali bent jau pradėti spręsti problemą rimčiau, nei ištardami įprastinę mantrą: „Ar mėginote perkrauti sistemą?“

Dabar mes atsidūrėme tokioje situacijoje, kai tik šis negausus elitas (vadinkite juos kompiuterių fanatikais, technokratais, programišiais, koduotojais ar kaip kitaip) nuodugniai supranta technologijas, kurios su kiekviena diena vis intensyviau ir plačiau valdo mūsų gyvenimą, o dauguma mūsų absoliučiai nieko apie tai neišmano. Pradėjau vertinti šio reiškinio svarbą, nagrinėdamas medžiagą savo ankstesnei knygai apie pasaulinį organizuotą nusikalstamumą *McMafia*. Nuvykau į Braziliją, norėdamas ištyrinėti kibernetinius nusikaltimus, nes ši viliojanti šalis, be daugelio savo teigiamų ypatybių, yra pagrindinis visokių internete vykstančių blogybių centras. Nors tuo metu apie tai buvo mažai žinoma.

Ten sutikau kibernetinių vagišių, kurie buvo sukūrę nepaprastai sėkmingą kompiuterinio sukčiavimo būdą, angliškai vadinamą *phishing scam**. Šios rūšies sukčiavimas vis dar sudaro pačią svarbiausią internetinių nusikaltimų dalį. Egzistuoja du paprasti variantai. Auka atidaro nepageidaujamą, iš nežinomo adresato gautą elektroninį laišką. Laiško priede (angl. *attachment*) gali būti atsiunčiamas virusas, kuris leidžia kur nors kitoje pasaulio vietoje esančiu kompiuteriu kontroliuoti viruso pažeistą kompiuterį, o kartu ir į jį įvedamus bankinius slaptažodžius. Kitas triukas yra sukurti tarsi iš banko ar kitos įstaigos atsiųstą elektroninį laišką, reikalaujantį patvirtinti prisijungimo ir slaptažodžio duomenis. Jei laiško gavėjas nepastebi klastos, tada sukčius, atsiuntęs laišką, šiuos duomenis gali panaudoti, norėdamas prieiti prie visų ar kai kurių laiško gavėjo internetinių sąskaitų. Brazilijos programišiai palaipsniui pasisavino dešimtis milijonų dolerių iš banko sąskaitų Brazilijoje, Ispanijoje, Portugalijoje, Jungtinėje Karalystėje ir Jungtinėse Amerikos Valstijose.

* Internetu pareikalauti konfidencialios informacijos, siekiant apgaulės būdu išvilioti kreditinių kortelių numerius, slaptažodžius ar kitus asmeninius duomenis. (Čia ir toliau vert. past.)

O paskui aš apsilankiau pas Brazilijos policininkus, kurie tiria kibernetinius nusikaltimus ir kurie buvo suėmę keturis nusikalstamos grupuotės narius (nors mažiausiai dvigubai tiek policija niekada taip ir nesugebėjo susekti), tada paėmiau interviu iš Amerikos kompiuterių saugumo kompanijos ISS slaptųjų operacijų skyriaus „X-Force" viršininko. Maždaug per savaitę aš supratau, kad nusikaltėliai, vykdantys įprastinius arba vadinamuosius tradicinius organizuotus nusikaltimus, kad ir kokie spalvingi ir įvairūs jie būtų, rizikuoja žymiai labiau nei tie, kurie dalyvauja kibernetiniuose nusikaltimuose.

Norėdamos sėkmingai veikti, seno kirpimo organizuotos nusikalstamos grupuotės, pripratusios prie dvidešimto amžiaus technologijų ir priemonių, turi įveikti dvi kliūtis. Pirminė jų verslo rizika susijusi su policija. Teisėsaugos priemonių efektyvumas skiriasi priklausomai nuo geografinės padėties ir laikui bėgant kinta. Organizuotos nusikalstamos grupuotės prisitaiko prie šių besikeičiančių sąlygų ir pasirenka kurį nors iš daugybės elgesio su teisėsaugos ir viešosios tvarkos palaikymo pajėgomis metodų: mėgina juos nugalėti arba papirkti, mėgina papirkti policiją valdančius politikus arba bando likti nesusektos. Tada jos susiduria su antra problema – grėsme dėl konkurencijos, kai kiti blogi berniukai ieško grobio tuose pačiuose vandenyse. Čia ir vėl galima bandyti įveikti konkurentus, galima pasiūlyti susivienyti arba sutikti pereiti pas juos.

Tačiau nė vienu atveju nusikaltėlių sindikatas negali paprasčiausiai ignoruoti šių kliūčių – taip padarius jų laukia nesėkmė, kartais su lemtingomis pasekmėmis. Norint išlikti ir klestėti, svarbiausia sugebėti bendrauti tiek su savo bendrais nusikaltėliais, tiek su policija – ir, be abejonės, abiem grupėms perduoti tinkamą informaciją.

Brazilijoje labai greitai įsitikinau, kad dvidešimt pirmo amžiaus nusikaltimai yra kitokie.

Svarbiausia, kad internete daug sunkiau nustatyti nedorų kėslų turinčius veikėjus. Internetą reguliuojantys įstatymai įvairiose šaly-

se labai skiriasi. Tai svarbus faktas, nes, apskritai paėmus, nusikalstamas veiksmas internete paprastai padaromas iš IP (internetinio protokolo) adreso vienoje šalyje prieš individą ar korporaciją kitoje šalyje, o įgyvendinamas (pinigai išgryninami) trečioje šalyje. Pavyzdžiui, policijos pareigūnas Kolumbijoje galbūt sugebės nustatyti, kad IP adresas, iš kurio koordinuojamas Kolumbijos banko užpuolimas, priklauso Kazachstanui. Tačiau paskui jis sužinos, kad Kazachstane tai nelaikoma nusikaltimu, taigi asmuo, einantis tokias pat pareigas Kazachstano sotinėje, neturės pagrindo tirti šio nusikaltimo.

Daugelis kibernetinių nusikaltėlių sugeba išnagrinėti šiuos prieštaringumus ir jais pasinaudoti. „Aš niekada nesinaudoju amerikietiškomis kreditinėmis ar debetinėmis kortelėmis, – pasakojo vienas iš labiausiai klestinčių Švedijos nusikaltėlių, vagiančių banko kortelių duomenis ir naudojančių juos apgaulingiems internetiniams sandėriams atlikti, – nes tada, būdamas bet kurioje planetos vietoje, tapčiau pavaldus Jungtinių Valstijų teisinei jurisdikcijai. Taigi renkuosi tik europietiškas ir kanadietiškas banko korteles. Tada jaučiuosi laimingas ir saugus, žinodamas, kad manęs niekada nesugaus."

Labai svarbu atskirti Jungtines Valstijas nuo Europos ir Kanados, nes pastarosiose kibernetinių aukų yra daugiausia. Ten galioja žymiai griežtesni įstatymai, apsaugantys asmeninę laisvę ir teises internete. Viena po kitos JAV vyriausybės suteikė teisėsaugai didesnių galių, nei ruošėsi suteikti dauguma Europos vyriausybių, ir motyvuodamos būtinybe kovoti su nusikalstamumu ir terorizmu leido pareigūnams lengviau prieiti prie privačių kompanijų duomenų.

Visa tai iš vienos pusės yra išmintinga, o iš kitos – sunkiai suvokiama, bent jau dabar, kai susirūpinimas dėl nusikalstamumo, įtariamųjų sekimas, privatumas, duomenų kaupimas tiek privačiose, tiek valstybinėse institucijose, kalbos laisvė („WikiLeaks" išviešinimas), lengva prieiga prie interneto svetainių (vadinamieji

internetinio neutralumo debatai) ir socialinė veikla interneto tinkluose kaip politinis įrankis kibernetinėje erdvėje nuolat susikerta su nacionalinio saugumo interesais.

Galbūt kas nors galėtų įrodinėti, kad, pavyzdžiui, visuotinis daugiaplatformis, daugiafunkcis internetinės paieškos sistemos „Google" prieinamumas pažeidžia Amerikos antimonopolinius teisės aktus ir kad visų tų asmeninių duomenų kaupimas yra parankus nusikaltėliams, o kartu kelia grėsmę piliečių laisvėms. Tačiau „Google" lengvai gali atkirsti, kad jos genialumo esmę ir sėkmę kaip tik ir sudaro jos daugiaplatformis, daugiafunkcis prieinamumas ir kad tai savaime skatina Amerikos komercinius ir saugumo interesus. Tik panorėjusi JAV vyriausybė per kelias valandas gali prieiti prie „Google" sistemos duomenų, naudodama legalias procedūras, o kadangi „Google" surenka duomenis iš viso pasaulio, tai suteikia Vašingtonui didžiulį strateginį pranašumą. Kitos vyriausybės apie tokią sėkmę gali tik pasvajoti. Kitaip nei kolegos iš Kinijos, Rusijos ar Vidurio Rytų šalių, amerikiečių vyriausybės atstovams nereikia brautis į kompiuterinę „Google" sistemą, norint ištyrinėti jos paslaptis. Jie paprasčiausiai gali gauti teismo orderį. Argi verta to atsisakyti dėl antimonopolinių teisės aktų?

Internetas – tai didelio burbulo teorija: išsprendus vieną jo problemą, kur nors kitur staiga iškyla kita, ne lengviau išsprendžiama. O didžiausia problema teisėsaugai yra anonimiškumas.

Šiandien kiekvienam, išmaniai besinaudojančiam internetu ir gebančiam mokytis, vis dar išlieka puiki galimybė nuslėpti fizinę kompiuterio buvimo vietą.

Egzistuoja du pagrindiniai būdai, kaip tai padaryti – pirmoji kibernetinė siena yra vadinamasis virtualus privatus tinklas VPN (angl. *Virtual Private Network*), kur grupė kompiuterių gali turėti vieną ir tą patį IP adresą. Paprastai IP adresas yra priskiriamas vienam kompiuteriui, bet, naudojant virtualų privatų tinklą, gali

atrodyti, kad keletas kompiuterių visai skirtingose pasaulio vietose yra, pavyzdžiui, Botsvanoje.

Tie, kurių netenkina virtualaus privataus tinklo apsauga, gali pasistatyti kitą kibernetinę sieną, naudodamiesi vadinamaisiais įgaliotaisiais serveriais (angl. *proxy server*). Seišeliuose esantis kompiuteris gali naudoti įgaliotinį, tarkim, Kinijoje ar Gvatemaloje. Įgaliotasis serveris neatskleidžia, kad pirminis IP perduoda informaciją iš Seišelių, juo labiau kad kompiuteris priklauso virtualiam privačiam tinklui, esančiam, tarkim, Grenlandijoje.

Visi šie nustatymai nereikalauja itin aukšto lygio kompiuterinių įgūdžių, taigi tokiais metodais daugiausia naudojasi tik dvi kibernetinių nusikaltėlių grupės: tikri įsilaužėliai į kompiuterių sistemas ir tikri kriminaliniai nusikaltėliai. Tačiau šie aukštos klasės operatoriai, atstovaujantys naujam rimtų organizuotų nusikaltimų tipui, sudaro tik mažumą visų, dalyvaujančių kompiuteriniuose nusikaltimuose.

Dar lieka smulkūs žaidėjai, veikiantys individualiai ir operuojantys palyginti mažomis grynųjų pinigų sumomis; jų, kai šitaip trūksta teisėsaugos pajėgų, nelabai ir verta gaudyti. Net jei šie veikėjai ir nesivargina pasinaudoti virtualiais privačiais tinklais, įgaliotaisiais serveriais ar daugybe kitų slapstymosi metodų, jie vis tiek gali labai apsunkinti policijos pareigūnų gyvenimą, užšifruodami savo ryšius.

Programinė įranga, kuri garantuoja jūsų užrašytos (netgi balso ar vaizdo) informacijos šifravimą, lengvai ir nemokamai prieinama internete, o žinomiausia yra PGP, šnekamojoje kalboje vadinama „Pretty Good Privacy“*.

Šifravimas yra galinga priemonė, kuriai kibernetinėje apsaugoje tenka svarbus vaidmuo. Tai kalbos „sujaukimas“, naudojant skaitmeniniu būdu generuojamus šifro raktus, kurių kombinacijos yra

* Pakankamai geras privatumas. (Angl.)

tokios matematiškai sudėtingos, kad gali būti atskleistos tik žinant slaptažodį. Šiuo metu užšifruoti dokumentai iš esmės tebėra saugūs, nors Vašingtonui priklausanti Nacionalinio saugumo agentūra (NSA), galingiausia pasaulio skaitmeninio šnipinėjimo tarnyba, nuolatos ieško būdų, kaip juos iššifruoti. Tarp kibernetinių nusikaltėlių jau plačiai sklinda gandai, kada NSA ir jos žvalgybos partneriai Kanadoje, Britanijoje, Australijoje ir Naujojoje Zelandijoje turi galimybių įsilaužti į šias viešas šifravimo sistemas, pasinaudodami savo „Orwellian Echelon" sistema. Buvo pranešta, kad ši sistema turi prieigos telefoną, elektroninį paštą ir palydovinį ryšį bet kurioje pasaulio vietoje.

Skaitmeninio šifravimo politinė reikšmė yra tokia didelė, kad Jungtinių Valstijų vyriausybė praeito amžiaus paskutiniame dešimtmetyje šifravimo programinę įrangą pradėjo klasifikuoti kaip „ginkluotę", o Rusijoje, jei policija ar KGB rastų nors vieną šifruotą failą jūsų kompiuteryje, jums galėtų būti priteisti keleri metai kalėjimo, net jei dokumente būtų tik jūsų savaitinių pirkinių sąrašas. Kadangi vyriausybės ir korporacijos sukaupia kas kartą vis daugiau asmeninės informacijos apie savo gyventojus ir klientus, jos užšifravimas tebėra viena iš kelių apsaugos priemonių, likusių individams savo privatumui išsaugoti. Tai taip pat yra neįkainojamas instrumentas tiems, kurie užsiima nusikalstama veikla internete.

Lygiai kaip tradiciniai kriminaliniai nusikaltėliai turi susikurti tarpusavio bendravimo būdus, kad galėtų nustatyti draugus, priešus, policininkus ar konkurentus, taip ir kibernetiniai piktadariai susiduria su nuolatiniais iššūkiais, mėgindami nustatyti, kas iš tikrųjų yra kiekvienas asmuo, su kuriuo jie bendrauja internetu. Dalis šioje knygoje išdėstytos istorijos pasakoja apie tai, kaip jie ištobulino vieni kitų atpažinimo metodus ir kaip policijos pajėgos visame pasaulyje stengiasi įveikti programišių sugebėjimą internete atpažinti

teisėsaugos atstovus ir vadinamuosius konfidencialius informatorius (angl. *Confidential Informants*, sutr. CIs).

Per praeito amžiaus paskutinį dešimtmetį paprasčiausias būdas užkirsti kelią nepageidaujamiems svečiams, norintiems kišti nosį į nusikaltėlių veiklą, buvo griežtos vetavimo ir narystės sistemos įvedimas interneto svetainėse, skirtose internetiniams nusikaltimams aptarti. Nepaisant šių saugumo priemonių, vos po kelių mėnesių tokios teisėsaugos institucijos kaip Jungtinių Valstijų slaptoji tarnyba ar tokios žvalgybos tarnybos kaip KGB įpėdinė FSB*, gavusios prieigą, jau naršė po visas interneto svetaines, kantriai apsimetinėjo nusikaltėliais arba įkalbėdavo informatorius dirbti jų naudai.

Buvo agentų, veikiančių taip įtikinamai, jog kai kurios teisėsaugos tarnybos netgi skyrė tam tikrą savo išteklių dalį persekioti slaptiesiems policijos pareigūnams iš gimininingų organizacijų, nes spėjo, kad jie yra tikri nusikaltėliai.

Policijos pajėgos ir šnipai per pastarąjį dešimtmetį savo pastangomis surinko didelę programišių – kriminalinių nusikaltėlių duomenų bazę: jų pravardes, jų tikrąsias ar numanomas buvimo vietas, veiklos, į kurią jie yra įsitraukę, pobūdį, informaciją apie tai, su kuo jie dažniausiai bendrauja. Žemiausio lygmens kibernetiniai nusikaltėliai iki minimumo sumažino duomenų kiekį. Tačiau, nepaisant viso šito, vis dar tebėra nepaprastai sunku patraukti kibernetinius nusikaltėlius baudžiamojon atsakomybėn.

Būtent pati interneto prigimtis, ypač jo tarpusavio ryšių galimybė, ir sukelia teisėsaugos ir teisėtvarkos pajėgoms didžiulį galvos skausmą: niekas nėra šimtu procentų tikras, su kuo jis bendrauja internetu. Ar turit reikalų su paprastu, eiliniu programišium, vykdančiu nusikalstamą veiklą? Ar su kuo nors, kas turi „aukščiau sėdinčių"

* *Федеральная служба безопасности Российской Федерации* – Rusijos Federacijos federalinė saugumo tarnyba. (Rus.)

draugų? Ar su nusikaltėliu? Ar su šnipu? O gal su kariniu tyrėju, kurio tikslas – įvertinti nusikalstamo įsilaužimo į sistemas metodus? Ar jūs stebite savo pašnekovą, ar jis stebi jus? Ar jis bando užsidirbti pinigų sau? Ar „Al-Qaidai"?

„Tai tarsi žaidimas septynmačiais šachmatais, – įvertino futurologas Bruno Guissani, – kuriame niekada nesate tikras, kas bet kurią akimirką yra jūsų oponentas."

Atvykęs į „Google" būstinę, esančią Mauntin Vju, Kalifornijoje, neprarandi žado, kaip pirmą kartą pamatęs Tadž Mahalą, tačiau, pastatęs savo automobilį Čarlstono aveniu priešais įvairiaspalvį ženklą, skelbiantį apie vieną iš poindustrinio pasaulio stebuklų, aš visgi pajutau pagarbią baimę.

Greitis, kuriuo „Google" įsiskverbė į mūsų sąmonę, su visomis sėkmėmis ir nesėkmėmis, siejamomis su narkotinių medžiagų kontrole, neturi precedento. Jos vieninteliai konkurentai –tokie skaitmeniniai milžinai kaip „Facebook", „Microsoft" ir „Amazon" – tai tos pačios šeimos pusbroliai ir pusseserės. Bet net ir šie trys milžinai, padėdami mums, vadovaudami mūsų gyvenimui ir kontroliuodami jį, negali pasigirti tokia sėkme kaip „Google", nes jos didžiuliai, „giliai įsirausę" serveriai išmeta nesuskaičiuojamą daugybę reikalaujamos informacijos baitų, tuo pat metu siurbdami ir kaupdami milijardų žmonių individualius ir kolektyvinius duomenis. Šie duomenys neabejotinai atskleidžia apie mus daug daugiau, nei patys apie save žinome. Šiurpulys ima vien pagalvojus, kas galėtų nutikti, jei informacija patektų į blogas rankas. O gal jau ir pateko...

Žaismingas pagrindinių ir antrinių pastelinių spalvų mišinys, gerai pažįstamas iš „Google" logotipo, yra atkartotas „miestelio" teritorijoje. Aplinkui tarsi netvarkingai, bet iš tiesų preciziškai išdėlioti dideli daiktai, dažnai išsiskiriantys neaštriais užapvalintais kraštais. Skulptūros suprojektuotos taip, kad ant jų būtų galima sė-

dėti, į jas žiūrėti arba su jomis žaisti, taigi visas kompleksas panašus į milžinišką vaikų darželį arba, priklausomai nuo jūsų nerimo ar paranojos lygio, į keistą žaislinį kaimelį iš praeito amžiaus septinto dešimtmečio TV šou „Kalinys" – kaimelį, į kurį rizikingai buvo pasiųsti nacionalinio saugumo darbuotojai ir iš kurio buvo neįmanoma pabėgti. Ar man tik taip atrodo, ar iš tiesų visi, kuriuos mačiau tame miestelyje, pradedant valytojomis ir baigiant vyresniąja vadovybe, šypsosi, lyg būtų apimti transo? Tai sustiprina paranojišką „Google" interpretaciją, o kartu sudaro įspūdį, kad jie kiek per smarkiai stengiasi neatrodyti blogiukai. Net negaliu tiksliai pasakyti, ar tai panašiau į svajonę, ar į košmarą.

Susitikęs su „Google" Pasitikėjimo ir saugumo tarnybos viršininku Corey Louie, pajuntu tam tikrą palengvėjimą, nes paprastai žmonės, dirbantys saugumo tarnybose, pasižymi dalykiška veido išraiška ir yra linkę į slaptumą, nepriklausomai nuo to, kam dirba. Jo manieros sudaro malonų kontrastą tai ypatingai budistinei „Google" atmosferai. Tai sumanus, judrus ir gerų manierų daugiau nei trisdešimties azijietiškos kilmės amerikietis, kuris savo patirtį įgijo ne tarp tingių Silicio slėnio* svajotojų, bet žymiai šiurkštesniame, vyriškesniame Jungtinių Valstijų slaptosios tarnybos pasaulyje. Jis buvo priimtas į „Google" 2006 m. pabaigoje, pustrečių metų prieš man apsilankant. O iki tol, kol išėjo iš teisėsaugos, Corey Louie vadovavo Slaptosios tarnybos Elektroninių nusikaltimų skyriui. Beveik nėra to, ko jis nežinotų apie internetines atakas (vadinamuosius įsibrovimus arba įsiskverbimus), sukčiavimus su kreditinėmis kortelėmis, plačiai plintantį paskirstytą atsisakymą

* Silicio slėnis (angl. *Silicon Valley*) – pietinė San Fransisko (Kalifornija) įlankos dalis, kur įsikūrusios daugelis didžiausių pasaulyje technologinių korporacijų. Anksčiau terminas buvo vartojamas regiono silicio mikroschemų gamintojams apibūdinti, o dabar nusako visas aukštųjų technologijų (angl. *high-tech*) verslo įmones šioje teritorijoje.

aptarnauti DDoS (angl. *Distributed Denial of Service*), galintį išvesti iš rikiuotės interneto svetaines ir tinklus, ir apie kenkėjiškas programas, kurios, vos tik peržengus tūkstantmečio slenkstį, pradėjo daugintis tarsi žiurkės kanalizacijoje. Be to, jis daug žino apie kasdienę kibernetinių nusikaltėlių duoną – pavogtų arba įsibrovus į kompiuterinę duomenų bazę nuskaitytų kreditinių kortelių duomenų pirkimą ar pardavimą. Šimtais tūkstančių šių duomenų keičiamasi visame pasaulyje, o paskui jais naudojamasi prekėms pirkti arba gryniesiems iš bankomatų pasiimti.

Kaip „Google" galėjo atsispirti tokiai turtingai strateginei patirčiai, kokią turi Corey Louie? Žinoma, negalėjo. O kaip Louie galėjo atsispirti strateginiam karjeros šuoliui į „Google" – ir švelniam Jungtinių Valstijų pietinės Ramiojo vandenyno pakrantės klimatui, lyginant jį su Kolumbijos apygardos drėgme, žiemos šalnomis ir tik viena savaite vyšnių žydėjimo; taip pat Vakarų pakrantės kasdieniam aprangos kodui, lyginant jį su standžiomis Beltvėjaus* apykaklėmis; pinigams ir pojūčiui, jog dalyvauji dinamiškame JAV vyriausybinių tarnybų projekte? Kova iš tiesų nelygi. Važiuojant 101-uoju greitkeliu iš San Fransisko, „Google" nėra vienintelis kibernetinės kompanijos ženklas, kurį pastebite: „Sun Microsystems", „Yahoo!" ir „McAfee" – tai tik kelios iš daugelio įžymių kompanijų, kurių būstines regite pro automobilio langus, keliaudamas pietų kryptimi. Kuo daugiau kompanijų aplankote, norėdamas aptarti saugumo problemas, tuo daugiau sutinkate buvusių vyriausybinių agentų iš FTB, Jungtinių Valstijų slaptosios tarnybos USSS (angl. *United States Secret Service*), CŽV, Kovos su narkotikais administracijos DEA (angl. *Drug Enforcement Administration*) ir JAV pašto inspekcijos tarnybos USPIS (angl. *United States Postal Inspection Service*). Visas

* Vašingtono politinių įstaigų rajonas, kuriame sutiksite daugybę federalinių pareigūnų, lobistų, konsultantų ir žiniasklaidos komentatorių.

būrys buvusių šnipų ir slaptosios policijos pareigūnų emigravo iš nesveikos Vašingtono aplinkos, ieškodami geresnio gyvenimo Silicio slėnyje, sugundyti tų pačių puikių sąlygų, kurios kino pramonės atstovus atviliojo į Holivudą.

Šio nutekėjimo iš valstybinių agentūrų į privatų sektorių padariniai yra aiškiai nuostolingi vyriausybei. Iždo pinigai investuojami į kibernetinių tyrėjų mokymą, o šie, įgiję kelerių metų patirtį, išvyksta į malonesnio klimato vietas. Vis dėlto šis investavimas nėra visai bergždžias, nes dėl jo sutvirtėjo galingi ryšiai tarp viešojo ir privataus sektorių. „Google" nėra tik privati korporacija. Baltųjų rūmų požiūriu, tai strateginis nacionalinis turtas. Iš Vašingtono perduodama gana aiški žinia – atakuodami „Google", jūs atakuojate JAV. Todėl tai, kad toks žmogus kaip Corey Louie gali paimti telefoną, pasikalbėti su savo senais bičiuliais iš Slaptosios tarnybos ir įspėti juos, tarkim, apie didžiulį „Gmail"* užpuolimą, labai palengvina svarbų viešojo ir privataus sektorių bendradarbiavimą internetinio saugumo klausimais.

Nesu tikras, tačiau galiu lažintis, kad Corey gyvenimo lygis pagerėjo nuo tada, kai jis išvyko į vakarus, bet jam tenka itin sunkiai dirbti. „Google" yra viena iš dviejų didžiausių duomenų saugyklų pasaulyje – kita yra „Facebook". Kaip tik dėl to šios kompanijos yra tokios patrauklios (reklamuotojai noriai moka už žmonių asmeninių įpročių paslaptis, kurias atskleidžia šie duomenys), o kartu jos yra tikras lobis programišiams, dirbantiems sau, pogrindinėms organizacijoms, pramonei ar konkuruojančioms valstybėms.

Mūsų pokalbiui su Corey artėjant į pabaigą, jis man papasakojo apie savo draugą policininką, kuris daug laiko paskyrė tam, kad susidraugautų su programišiais. Jam taip gerai sekėsi, kad jis perėmė didžiulės kriminalinės svetainės internete administravimą.

* Nemokama, iš reklamų remiama elektroninio pašto tarnyba.

„Galbūt jam būtų malonu pasikalbėti su jumis, – pasakė Corey. – Jis tvarkė interneto svetainę, vadinamą „DarkMarket“ (Tamsioji rinka).“ Tai buvo pirmas kartas, kai aš išgirdau apie šitą svetainę ir apie specialųjį FTB agentą Keithą J. Mularskį. Taip prasidėjo mano keista kelionė.

Išsiruošiau susitikti su kuo daugiau po įvairias šalis išsisklaidžiusių Tamsiosios rinkos pagrindinių veikėjų – vagių, policininkų, dvigubų agentų, teisininkų, programišių, įsilaužėlių į kompiuterius ir proziškesnių nusikaltėlių – ir paimti iš jų interviu. Ieškodamas informacijos taip pat peržiūrėjau daugybę teismų dokumentų, susijusių su Tamsiąja rinka ir jos dalyviais. Buvę ir esami kibernetiniai nusikaltėliai ir policijos pareigūnai pateikė man papildomų dokumentų ir informacijos. Aš taip ir nesugebėjau prieiti prie viso pačios svetainės archyvo, bet man pavyko pasklaidyti nemažą jo dokumentų dalį. Agentas Mularskis, turintis beveik visą Tamsiosios rinkos archyvą, yra vienintelis iš mano sutiktųjų, susijusių su šiuo reikalu, galėjęs naudotis visais tais dokumentais savo nuožiūra.

Be sunkiai prieinamo archyvo, buvo ir kai kurių kitų dokumentinių liudijimų. Pastarieji, nors ir naudingi, dažnai buvo netikslūs. Tai ypač pasakytina apie medžiagą, kurią kaltintojai pateikė daugelyje teismo procesų. Mano nuomone, šie netikslumai nebuvo nei susiję su nerūpestingumu ar kerštingumu, nei tyčiniai. Veikiau jie atspindėjo aukšto techninio lygio ir dažnai painią su kibernetika susijusių bylų parodymų prigimtį. Teisėjai ir advokatai dėjo visas pastangas, norėdami perprasti šią specifinę kultūrą, lygiai taip kaip daro visi kiti, pirmą kartą susidūrę su internetinėmis piktadarybėmis.

Taigi ši istorija iš esmės yra susijusi su joje dalyvaujančiais veikėjais ir jų veiksmais. Šie liudijimai, be abejo, daugiausia paremti jų asmeniniais prisiminimais, apimančiais visą pastarąjį dešimtmetį. Gerai žinoma, kad prisiminimai dažnai būna klaidingi, be to, visi

dalyvaujantys veikėjai turėjo savų tikslų, siekdami išryškinti vienus savo veiklos Tamsiojoje rinkoje momentus ir nuslėpti kitus. Čia jiems padėjo bendravimo internetu dviveidiškumas ir pati kultūra, kurioje tiems, kurie meluoja ir maskuojasi, galima pritaikyti labai nedaug sankcijų.

Mano pastangos įvertinti, kada apklausiamas asmuo meluoja, pagražina faktus ar fantazuoja, buvo tik iš dalies sėkmingos. Visi, iš kurių ėmiau interviu, trykšte tryško protu, nors kai kuriems ir trūko tvirto moralinio principingumo, kuris reikalingas norint išsklaidyti drumstus kibernetinio nusikalstamumo vandenis. Bet vis labiau ir labiau gilindamasis į paslaptingą Tamsiosios rinkos pasaulį, aš supratau, kad skirtingi tų pačių siužetų apie šios interneto svetainės istoriją variantai iš esmės buvo prieštaringi ir nesuderinami. Buvo neįmanoma tiksliai nustatyti, kas iš tiesų vyksta tarp žaidėjų ir su kuo jie galų gale dirba.

Internete sukurtos beribės duomenų ir informacijos saugyklos, didžiulis procentas jų yra bevertės, dauguma tebėra mažai kam įdomios ir tik mažuma yra pavojingos dėl savo melagingumo. Augant mūsų priklausomybei nuo tinklinių sistemų ir jų tarpusavio ryšių, kai tokios labai specializuotos grupės kaip nusikaltėliai programišiai ir žvalgybos agentai gali dalyvauti tiek nusikalstamoje veikloje, tiek pramoniniame šnipinėjime ar kibernetiniuose karuose, mėginimas suprasti ir dokumentais pagrįsti tokių reiškinių kaip Tamsioji rinka istoriją tapo gyvybiniu intelektualiniu ir socialiniu uždaviniu, net jei įrodymai yra neišsamūs, tendencingi ir išsibarstę tiek realiame, tiek virtualiame pasauliuose.

PIRMA KNYGA

I dalis

1
Skambina inspektorius

Jorkšyras, Anglija, 2008 m. kovas

Vieną ankstyvą 2008 m. kovo pradžios rytą pastorius Andrew Arunas Johnas patyrė lengvą šoką. Sunku jį kaltinti. Jis ne tik buvo ką tik atlaikęs ilgą kelionę iš Delio galvijų vagono lygio klase. Ši kelionė įvyko prieš dvi savaites iki atidarant naują, penktąjį Hitrou oro uosto terminalą, taigi judriausias tarptautinis oro uostas nagrinėjo naujus standartus keleivių vargams palengvinti. Pastoriaus skrydis iš Indijos prasidėjo apie trečią valandą nakties ir, įveikus pasų kontrolės postą ir bagažo atsiėmimo chaosą, jo dar laukė keturių valandų kelionė automobiliu šiaurės kryptimi į Jorkšyrą.

Įsijungęs mobilųjį telefoną, pastorius Johnas pamatė daugybę praleistų žmonos skambučių. Nespėjus paskambinti jai ir pasiteirauti, dėl ko taip nerimauja, vėl suskambo telefonas. Ji pasakė, kad keletą kartų skambino iš policijos, žūtbūt norėdami su juo susisiekti.

Nustebintas ir sutrikęs kunigas atkirto žmonai, kad ji kalbanti nesąmones – nors tuoj pat pasigailėjo savo balso tono.

Laimei, žmona nekreipė dėmesio į jo irzlumą. Ji aiškiai ir ramiai išdėstė, kad policija norinti įspėti jį, jog kažkas įsilaužė į jo

banko sąskaitą, kad reikalas skubus ir kad jis kuo greičiau paskambintų atsakingam pareigūnui jos turimu numeriu.

Žmonos skambutis dar labiau sutrikdė pastorių ir jo jau ir be to pavargusios smegenys dar labiau įsiaudrino. „Kas įsilaužė į mano sąskaitą? – stebėjosi jis. – Kokią sąskaitą? Mano „Barclays" banko sąskaitą čia? – svarstė jis. – Ar mano „Standart" banko sąskaitą Pietų Afrikoje? Ar mano sąskaitą ICICI banke Indijoje? O gal į visas tris? Ir dar mįslingiau: ką ji iš tiesų norėjo pasakyti? *Kaip* jie įsilaužė į mano sąskaitą?"

Kadangi tai įvyko tuoj pat po varginančios kelionės, visas šis reikalas privertė pastorių sunerimti ir suerzino jį. „Sutvarkysiu vėliau, kai parvyksiu į Bradfordą ir būsiu pailsėjęs", – sumurmėjo jis sau po nosimi.

Bradfordas yra už 200 mylių į šiaurę nuo Hitrou oro uosto. Šešiasdešimt mylių į rytus nuo miesto išsidėstęs Skantorpas, kur maža detektyvo seržanto Chriso Dawsono komanda nervindamasi laukė pastoriaus Johno telefono skambučio. Pareigūnas jautėsi, tarsi klimptų į kažkokį liūną, jo įtarimu, labai rimto reikalo liūną, kur susiduria su viena, regis, neįveikiama problema – jis čia nieko nevalioja suprasti. Tarp iki šiol surinktų įrodymų buvo šimtai tūkstančių kompiuterinių failų, ir kai kurie iš jų buvo tokie dideli, kad juose galėjo tilpti 350 kartų daugiau informacijos, nei užima visi Shakespeare'o kūriniai. Šiuose dokumentuose buvo sukaupta kosminė skaičių ir pranešimų biblioteka tokia kalba, kurios iš tiesų negalėjo iššifruoti niekas, išskyrus mažą visame pasaulyje išsisklaidžiusį elitą žmonių, suprantančių paslaptingą kibernetinių nusikaltimų terminologiją.

Detektyvas seržantas Dawsonas galbūt ir nieko neišmanė apie šią naują ir labai siauram ratui suprantamą kriminalinių tyrimų sritį, tačiau jis buvo pirmos klasės žmogžudysčių skyriaus pareigūnas su ilgamete tarnybos patirtimi. Tarp begalinių sąrašų ir skaičių eilučių

jis sugebėjo atsekti įslaptintus duomenis, kurie iš pažiūros tarsi ir neturėtų priklausyti vienam asmeniui.

Visgi, kaip dvidešimt pirmo amžiaus pirmame dešimtmetyje suprato daugelio pasaulio šalių policijos pareigūnai, egzistavo vienas dalykas, trukdantis darbui su šiais informacijos lobynais. Norint priskirti juos prie aiškiai apibrėžtų nusikaltimų, reikėjo visai kitokių, nei įprasta, būdų.

Jeigu detektyvas Dawsonas būtų bandęs įtikinti miegančio Skantorpo miestelio, esančio prie Hamberio upės žiočių, teismo pareigūnus leisti jam sulaikyti įtariamąjį kardomajam kalinimui, jam būtų reikėję neabejotinų aiškaus nusikaltimo įrodymų. Dar daugiau, buvo nemaža tikimybė, kad anksčiau aptartus įrodymus jis pateiks kokiam nors nukriošusiam senam išvažiuojamojo teismo teisėjui, kuris galbūt sunkiai susigaudo, ką veikti su nuotoliniu televizoriaus pulteliu, o ką jau kalbėti apie elektroninį paštą. Įsitikinimo nepakako – atvejis turėjo būti aiškiai ir kuo paprasčiau pagrįstas, kad kiekvienas galėtų jį suprasti.

Laikas tirpo. Įtariamasis galėjo būti sulaikytas trims dienoms, iš kurių dvi jau buvo praėjusios. Tarp visų tų failų, skaičių, pokalbių ir tinklalapių išklotinių ir dar galai žino ko Dawsonas turėjo tik vieną nedidelį pluoštelį įrodymų.

Jis įdėmiai žiūrėjo į penkiasdešimt žodžių A4 formato popieriaus lape. Ten buvo sąskaitos numeris: 75377983, sąskaitos atidarymo data: 2006 m. vasario 24 d., ir sąskaitos likutis: 4 022,81 svarų. Bet ten taip pat buvo ir pavardė: *Mr. A. A. John*; elektroninio pašto adresas: STPAULS@LEGEND.CO.UK; gyvenamosios vietos adresas: *63 St Paul's Road, Manningham, Bradford*; asmens registracijos kodas, o svarbiausia – registracijos slaptažodis: 252931.

Jei tik jis galėtų patvirtinti sąskaitos savininko tapatybę ir jei šis žmogus garantuotų, kad niekada sąmoningai neatskleidė savo slaptažodžio, tada Dawsonas galbūt sugebėtų įtikinti teisėją perduoti

kaltinamąjį teismui, neišleidžiant jo už užstatą. Taip detektyvas seržantas galėtų laimėti pakankamai laiko, kad tikrai perprastų, su kuo turi reikalą.

Kai Dawsonas pamėgino susisiekti su misteriu A. A. Johnu, jis sužinojo, kad šis yra Anglijos bažnyčios dvasininkas, išvežęs grupę neturtingų šeimų vaikų atostogauti į Indiją. Jam taip pat buvo pranešta, kad su pastoriumi nebus galima susisiekti, kol jis negrįš iš Delio. Pagal grafiką dvasininkas turėjo atvykti keliomis valandomis anksčiau, nei įtariamasis turėjo būti paleistas. Jeigu jis neatvyktų laiku, tada šios bylos liūnas prarytų aibę duomenų, kuriuos Dawsonas netikėtai aptiko. Pražūtų ne tik duomenys – įtariamasis neabejotinai vėl susilietų su savo virtualiuoju *alter ego*.

Dawsonui nepasisekė, kad pokalbis telefonu su žmona gerokai sutrikdė pastorių Johną ir kad jis apsisprendė sutvarkyti šį reikalą, kai bus parvykęs į savo parapiją Maningame. Pastorius iš tiesų išjungė savo mobilųjį telefoną ir susikaupė ilgai kelionei iš oro uosto.

Visgi kodėl jis buvo toks nusiminęs?

Trumpai ir glaustai sakant, pastorius Johnas pagal temperamentą buvo linksmas, geraširdis žmogus. Jis gimė Indijos Radžastano valstijoje, Taro dykumos pakraštyje. Jo kampuotas veidas paprastai švietė taip, lyg saulė spinduliuotų pro jo profesoriškus akinius. Jo gyvenimas prasidėjo Indijos krikščionių bendruomenėje, kuriai priklausė mažuma tikinčiųjų. Jis pasirinko dvasininko darbą Indijos anglikonų bažnyčioje Delyje, kur ištarnavo penkiolika metų.

Tačiau 1996 m. Pietų Afrikos provincijos bažnyčia* pereinamuoju nuo apartheido prie daugiapartinio valdymo laikotarpiu paskyrė jį vadovauti Lenasijos miestelio, esančio už trijų mylių į pietus nuo Soveto, parapijai.

Tai buvo sudėtingas persikėlimas, nes laikai nebuvo palankūs įsikurti naujuose namuose. Džiaugsmą, su kuriuo buvo sutikta ra-

* Nuo 2006 m. vadinama Pietų Afrikos anglikonų bažnyčia.

sistinio režimo baigtis, temdė suvokimas, kad pasipiktinimas, susikaupęs per pastaruosius 200 metų, įsigraužęs labai giliai. Tokiems pašaliečiams kaip pastorius Johnas reikėjo išlavintų politinių ir socialinių įgūdžių, norint suprasti egzistuojančios įtampos prasmę ir galbūt padėti ją sumažinti.

Jo sėkmingą darbą Pietų Afrikoje pastebėjo aukštesnioji Anglikonų bažnyčios vadovybė, ir po aštuonerių metų Bradfordo vyskupas iš Anglijos Vakarų Jorkšyro grafystės paragino jį apsvarstyti galimybę užimti tokį pat viliojantį postą Maningame, gyvenamajame rajone, esančiame netoli Bradfordo miesto centro. Pastorius Johnas delsė – Anglija su savo prastais orais ir išsidriekusiais miestais jam visada atrodė gana niūri.

Taip pat jis žinojo, kad Maningame jo laukia nelengvas gyvenimas. Daugelis britų laikė Bradfordą, o ypač Maningamą, nevykusių savo šalies pastangų suvienyti daugelį jos etninių ir religinių grupių simboliu. O piktavaliai matė Maningame galimybę padidinti nepasitikėjimą tarp šių bendruomenių.

2001 m. liepą šiame rajone kilo trumpos, bet įnirtingos riaušės, kurios atspindėjo gilėjantį susiskirstymą tarp didelės dalies azijiečių ir baltaodžių gyventojų. Dar anksčiau Maningamas buvo patyręs tokį reiškinį kaip „baltaodžių bėgimas"*, o kai praėjus trejiems metams po riaušių čia atvyko pastorius Johnas, 75 procentus gyventojų sudarė musulmonai, kurių dauguma buvo kilę iš šiaurės rytų Pakistano kaimiškųjų apylinkių. „Likę dvidešimt penki procentai yra krikščionys, nors gal tik kokie penki procentai iš jų lanko bažnyčią. Akivaizdu, jog baltųjų bendruomenė sudaro mažumą", – sakė pastorius Johnas. Nors Maningamo klimatas, architektūra ir kultūra nė kiek nepriminė Johanesburgo priemiesčių, kitais atžvilgiais jis turėjo kraupaus panašumo į Pietų Afriką.

* Didelio masto baltaodžių migracija iš įvairių rasių apgyvendintų miesto rajonų į rasiškai homogeninius priemiesčius ir užmiestį.

Tas paskyrimas reiškė sunkų išmėginimą. Kai susikaupė debesys ir iškrito sniegas, gatvės su niūrių naujosios gotikos stiliaus pastatų eilėmis tapo baisiai nepatrauklios. Nors šiek tiek daugiau nei prieš šimtmetį Maningamas buvo labai trokštama vieta gyventi. Tai buvo tuo išoriniam pasauliui jau užmirštu laikotarpiu, kai Bradfordas buvo pripažintas „pasauline vilnos sostine" ir galingu Britanijos pramoninės revoliucijos varikliu.

Tačiau prasidėjus dvidešimt pirmam amžiui Maningamą jau daugelį metų buvo apėmęs nuosmukis. Kadaise čia klestėję darbai ir gerovė jau seniai buvo nugrimzdę į praeitį. Jų vietą užėmė piktnaudžiavimas narkotikais, prievarta šeimyniniame gyvenime, turto vagystės ir prostitucija. Savo įsteigtame pagalbos centre pastorius Johnas sulaukdavo daugiau žmonių, bandančių pasislėpti nuo skurdo ir nusikalstamumo žabangų, nei jų susirinkdavo sekmadieniais į bažnyčią.

Tvyrant nuolatinei grėsmei, kad slepiamas smurtas gali prasiveržti į paviršių, pastoriaus Johno veikla atsidūrė Britanijos klasinių, kultūrinių ir socialinių karų priekinėse fronto linijose. Ne taip lengvai įbauginamas, iš daugelio aplinkybių jis tiesiog tylomis pasijuokdavo. Savo kasdieniame darbe jis visąlaik susidurdavo su iššūkiais, todėl dabar stebėjosi, kodėl jį taip smarkiai sutrikdė žinia apie pavojun patekusią jo banko sąskaitą. Pirmiausia jis norėjo pasikalbėti su savo sūnumis, išmanančiais apie kompiuterius. O tada nusprendė, kad jam reikia kuo greičiau kreiptis į policiją ir tiksliai išsiaiškinti, kas vyksta. „Svarbiausia, aš noriu, kad šis reikalas būtų kuo greičiau išspręstas ir užmirštas", – tvirtai pareiškė jis.

Nėra ko stebėtis nervinga pastoriaus reakcija. Psichologinis atsakas į žinią, kad tapai kibernetinio nusikaltimo auka, yra panašus į jausmą, patiriamą, kai tave apvagia. Nors šis veiksmas apsiriboja kibernetine erdve, taigi pasauliu, sudarytu iš mažų elektroninių impulsų, jausmas vis vien panašus į fizinę prievartą. Juk jei vagys įsi-

laužė į jūsų banko sąskaitą, kokią privačią informaciją jie dar galėjo rasti jūsų kompiuteryje?

Galbūt jie pavogė jūsų paso duomenis, ir koks nors nusikaltėlis arba žvalgybos agentas dabar naudoja juos padirbtiems kelionės dokumentams? Gal jie, kaip tenka skaityti, netgi tyrinėja jūsų elektroninio pašto žinutes su konfidencialia informacija apie kolegą ar bendradarbį? O gal jie atsitiktinai aptiko kokias nors pavojingas elektroninio flirto žinutes ar kitokią jūsų neapdairiai parašytą ar gautą informaciją? Ar yra kokia nors jūsų gyvenimo sritis, kurios jie nesugebėtų patyrinėti, galėdami prieiti prie jūsų kompiuterio?

Pastorius Johnas, dabar jau gana ryžtingai nusiteikęs, vos atvykęs į mažą jaukų namelį netoli savosios Maningamo bažnyčios su įspūdinga smaile, paskambino policijos pareigūnui į kaimyninę Linkolnšyro grafystę.

Tai, kad šis atvejis pakliuvo į Skantorpe dirbančio vidutinio amžiaus policininko Chriso Dawsono rankas, buvo labai neįprasta. Dauguma kibernetinių nusikaltimų bylų Britanijoje tenka specialistų grupėms, dirbančioms kurioje nors iš trijų institucijų – Metropoliteno policijoje, Londono miesto policijoje arba Sunkių organizuotų nusikaltimų agentūroje SOCA (angl. *Serious Organised Crime Agency*), taip pat įsikūrusioje sostinėje. Šioje srityje neįgudę pareigūnai paprastai negauna tokių bylų dėl jų ezoterinio pobūdžio. Tačiau Dawsonas nebuvo eilinis policininkas: jis turėjo puikią intuiciją ir buvo labai įžvalgus. Jis taip pat pasižymėjo ramiu žavesiu ir buvo nuoširdus, kas būdinga šiaurės Anglijos žmonėms, o visa tai prisidėjo prie jo metodiško ir preciziško požiūrio į teisėtvarkos palaikymą. Šis dėmesys smulkmenoms jam puikiai pravertė ateinančiais mėnesiais.

Maningamas siejamas su etnine įtampa ir staigiu ekonominiu nuosmukiu, o kaimyninis Skantorpas (turintis 75 000 gyventojų), esantis į pietus nuo Hamberio žiočių, dažnai vadinamas Anglijos

„niekur nesančiu miestu“ arba pajuokiamas tiek dėl savo pavadinimo*, tiek dėl nuolat prastai žaidžiančios futbolo komandos. (Teisingumo dėlei būtų galima pridėti, kad iki perkėlimo į žemesnę lygą 2011 m. gegužę miesto futbolo klubas „Scunthorpe United“, viršydamas savo galimybes, sužaidė antroje Anglijos futbolo lygoje). Kiek yra žinoma, miestas niekada nepasižymėjo plataus masto organizuotu nusikalstamumu.

Vos prieš keturias dienas iki pastoriui Johnui sugrįžtant iš labdaringos kelionės į Indiją detektyvas Dawsonas sėkmingai dirbo Skantorpo centrinėje policijos nuovadoje. Kompiuterio ekrane jis žiūrinėjo vadovavimo ir kontrolės žurnalą, kuriame registruojama informacija ir telefonu žmonių perduodami pranešimai apie nusikaltimus. Įprastiniai pranešimai būdavo apie girtuoklių peštynes, kartais šeimynines, arba kates, įstrigusias aukštai medžiuose. Bet tą trečiadienio popietę, pusę dviejų, registru perbėgo žinia, sužadinusi seržanto smalsumą. Tai buvo labai neįprastas pranešimas. Seržantas pasisuko į savo kolegą ir melodinga Linkolnšyro tarme ramiai pasakė: „Šįsyk geriau paskubėkim. Eime pažiūrėti. Atrodo, kad pas Grimley Smithą dedasi kažkas įtartino.“

* Pavadinimas susideda iš dviejų žodžių, kurių pirmasis žargonu reikštų purviną, šlykščią, bjaurią būtybę (paprastai mot. lyties), o antrasis – kaimą. Tai tarsi koks „padugnių ar kekšių kaimas“.

2
„Miranda“ praneša apie puikų naują pasaulį

Kompanijos „Grimley Smith Associates“ (sutr. GSA) interneto svetainėje puikuojasi tamsiai rusva jų pagrindinės buveinės nuotrauka iš karaliaus Edvardo laikų, kai čia veikė vienas iš pirmųjų Skantorpo automobilių salonų. Keista, kad kompanija išdidžiai reklamuoja „Belsize“, simbolizuojantį ankstyvuosius prabangius automobilius, kurių gamyba buvo nutraukta netrukus po Pirmojo pasaulinio karo. Tačiau šis garbus pirmtakas bei dikensiškas vardas ir pavardė Grimley Smith yra apgaulingi. Nes, kaip gerai žinoma, kompanija „Grimley Smith Associates“ buvo įkurta visai neseniai, 1992 m., ir ją įkūrė misteris Grimley ir misteris Smithas.

Kompanija siūlo daug sudėtingesnes technines paslaugas nei senų kledarų pardavimas ir remontas. Jos specializacija – chemijos inžinerijos pritaikymas energetikoje ir farmacijos pramonėje, ir ji yra laikoma viena iš sėkmingiausiai dirbančių neseniai įkurtų Skantorpo kompanijų, tokia, kuri gali didžiuotis pasaulinio lygio pripažinimu.

Du GSA įkūrėjai iš pradžių buvo ir vieninteliai kompanijos darbuotojai, o dabar joje dirba kelios dešimtys aukštos kvalifikacijos inžinierių. Kaip paprastai nutinka su visais verslais, kur sėkmė skatina plėtrą, GSA augimas buvo jaudinantis, tačiau nesistemingas. Kompanijos inžinieriai pasirašydavo sutartis dėl milžiniškų projektų tokiose tolimose šalyse kaip Iranas, Kinija ir Venesuela. Specifiniam jų darbo pobūdžiui ir tiksliems skaičiavimams, kur neleistina nė

mažiausia klaida, reikėjo galingų kompiuterinių programų. Jie ypač naudojosi kompiuterinio projektavimo programine įranga CAD*, leidžiančia modeliuoti sudėtingus projektus 2D ir 3D formatais.

2007 m. viduryje kompanija pasiekė tokią stadiją, kai jai žūtbūt reikėjo susitvarkyti kompiuterių infrastruktūrą. Pasitvirtino, kad patikėti jos priežiūrą ir saugumą kitoms bendrovėms brangiai kainuoja, be to, išaiškėjo, kad nuolat auga mokesčiai už visų kompanijos kibernetinių poreikių valdymą. Direktoriai nusprendė duoti nurodymą visą sistemą sutvarkyti naujais metodais.

Šiam darbui jie surado labai tinkamą gero būdo vietinį vaikiną Darrylą Leaningą. Jis pasižymėjo techninę kompetenciją, buvo jaunas, skrupulingai sąžiningas, bet galbūt svarbiausia buvo tai, kad jo laisvos, draugiškos manieros slėpė neįprastai aštrią nuovoką. Juk dažniausiai niekas per daug nesitiki, kad patys geriausi kompiuterių specialistai sugebės įveikti socialines ir psichologines problemas taip pat puikiai, kaip sugeba sutaisyti sudėtingus įrenginius.

Vos pirmą sykį įžengęs į biurą, Darrylas išsyk suprato, kad „Grimley Smith" kompiuterius reikia nedelsiant tvarkyti. Pagrindinį rūpestį jam kėlė tai, kad visi darbuotojai turėjo „administratoriaus teises". Į savo kompiuterius jie galėjo įdiegti bet kokias norimas programas ir naudotis bet kokiomis pasirinktomis interneto paslaugomis (išskyrus pornografiją, kuri ankstesniu Informacinių technologijų skyriaus nurodymu buvo centralizuotai uždrausta).

Šeimos kompiuteryje „administratoriaus" pareigas atlieka vienas asmuo (paprastai vienas iš tėvų). Pavyzdžiui, jis gali elektroniniu būdu apriboti laiką, kurį kiti šeimos nariai gali praleisti prie kompiuterio, gali parinkti interneto svetaines, kurias kitiems šeimos nariams leidžiama lankyti.

Viena iš svarbiausių „privilegijų", kurias šeimyniniai asmeniniai kompiuteriai suteikia administratoriui, yra susijusi su naujos progra-

* *Computer-aided design* – projektavimas kompiuteriu. (Angl.)

minės įrangos įdiegimu. Taip tėvai gali neleisti vaikams žaisti žaidimų, kuriuos laiko netinkamais. Bet jie taip pat gali naudotis šia privilegija, kad uždraustų įsikelti abejotinos kilmės programinę įrangą, nes tokios programos gali būti užkrėstos virusais ar kitokiais kenkėjais, dėl kurių visas šeimos skaitmeninis pasaulis taptų neapsaugotas nuo atakų.

Tie patys principai galioja ir verslo aplinkai, tik paprastai didesniu ir sudėtingesniu mastu. Pirmoji problema, kurią nustatė Darrylas, pradėjęs dirbti kompanijoje „Grimley Smith“, buvo centrinio administratoriaus nebuvimas. Direktoriams jis išaiškino, jog šiuolaikiniame versle nepateisinama, kad personalas gali parsisiųsti, įsikelti ar įsidiegti ką tik panorėjęs.

Darrylas jiems pasakė, kad centrinis valdymas yra esminis dalykas, norint išvengti tokių atvejų, kai virusai galėtų pažeisti kompiuterių tinklo apsaugą, ir pridūrė, kad darbuotojai greičiausiai yra visiškai patikimi. Antivirusines programas į sistemą reikia įdiegti ne todėl, kad įtariate, jog jūsų kolegos nori užkrėsti ją virusais, nes apskritai jie ir neturi tokių tikslų.

Tas pats pasakytina, aiškino jis, ir apie programinės įrangos įdiegimą bei, tiesą sakant, visa kita. Tokioje labai specializuotoje kompanijoje kaip GSA duomenų vertė yra iš esmės neįkainojama. Jei jie pakliūtų į blogas rankas, tai galėtų sužlugdyti kompaniją.

Savo kryžiaus žygyje, kurio tikslas buvo išvalyti „Grimley Smith“ kompiuterių sistemą nuo kenksmingų pažeidimų, Darrylas susidūrė su tam tikromis problemomis: tomis nematomomis skaitmeninėmis „skylėmis“, per kurias nepastebimi galėjo praslysti kompiuteriniai kirminai (angl. *worms*)*, trojanai** ir virusai. Pirmiausia jis suprato, kad

* Kompiuterinis kirminas – atskira savarankiška programa arba programų rinkinys, galintis platinti savo veikiančias kopijas arba jos dalis po kitas kompiuterio sistemas (dažnai per tinklą).

** Trojanas, arba Trojos arklys, yra programa, atliekanti nepageidautinus veiksmus be kompiuterio naudotojo žinios.

žmonės priešinsis, kai jiems reikės atsisakyti privilegijų, kuriomis, tegu ir negalėdami stebėti besiraičiojančių nuogų kūnų, GSA darbuotojai labai džiaugėsi. Nors ir būdamas jaunas specialistas, Darrylas visgi pademonstravo gerai išmanąs psichologiją, susijusią su kompiuterių naudojimu. Kažkaip jis turėjo atpratinti personalą nuo vietinių administravimo teisių. Jis nusprendė, kad geriausia tai padaryti palaipsniui. Žinodamas, kad žmonės paprastai nenori atsisakyti to, ką jau turi, jis išmąstė, kad lygiai taip pat jie mėgsta gauti naujų žaislų.

Taigi kai kitą kartą buvo atnaujinami kompiuteriai, jis pasinaudojo proga ir įvedė pirmuosius apribojimus. Džiaugdamiesi savo švytinčiais ir dar galingesniais naujaisiais kompiuteriais, GSA darbuotojai buvo pasirengę sutikti, kad nebegalės kada tik panorėję įsikelti į kompiuterius savo mėgstamiausių žaidimų ir laisvalaikio užsiėmimų.

Vėlgi demonstruodamas įgimtą psichologinį nuovokumą, Darrylas išvengė atvirai drakoniškų priemonių. Problemą sukėlė „Facebook“. Daugelis darbuotojų eikvojo kompiuterių išteklius, bendraudami socialiniame tinklalapyje darbo metu. Tačiau tai, anot saugumo specialistų, vis labiau virto vadinamuoju „užkrato pernešėju“, kitaip tariant, instrumentu, kurį virusų kūrėjai gali užpulti, norėdami paskleisti savo kūrinius.

Darrylas suprato, kad, visiškai uždraudus naudotis „Facebook“, gali kilti darbuotojų maištas, taigi leido naudotis šia interneto svetaine nuo 12 iki 14 val., kai dauguma žmonių pietauja. Pats nustatęs naudojimosi „Facebook“ laiką, jis galėjo padidinti kenkėjiškų programų ir pastangų įsilaužti į kompiuterius kontrolę ir užtikrinti, kad svetainė nekels pavojaus kompanijos saugumui.

Palaipsniui jis įdiegė sistemą su palyginti galinga centrine kontrole, neatstumdamas nė vieno „Grimley Smith“ kompiuterių naudotojo. Naujosios tvarkos pagrindą sudarė kompleksinė programa, vadinama „Virtualaus tinklo kompiuterija“, arba VNC (angl. *Vir-*

tual Network Computing). Tai buvo kompanijos „Grimley Smith“ nuosava „Didžiojo brolio“ versija. Nustatęs bet kokį neįprastą ar grėsmę keliantį elgesį tinkle, Darrylas galėjo paleisti VNC iš virtualaus įmygio ir nedelsdamas imti nuodugniai tirti, kas vyksta bet kuriame iš daugybės dabar jo valdomų kompiuterių.

Vieną rytą, kai personalas įsijungė kompiuterius, Darrylas išsiuntė žinutę, įspėdamas visus nuo generalinio direktoriaus iki žemiausio rango darbuotojo, kad nuo šiol bet kurį iš jų gali patikrinti kompiuterius prižiūrintis specialistas. Daugumai net nenutuokiant, Darrylo naujai įdiegta VNC smagiai dūzgė kaip foninė programa. Jei jis gaudavo perspėjimo signalą, kad kažkas parsisiuntė virusą ar bandė įdiegti kokią nors neatpažįstamą programinę įrangą, VNC būdavo aktyvuojama.

VNC yra labai galinga priemonė. Kai kam jos naudojimas gali pasirodyti kaip paprasta verslo praktika, tačiau globaliame internete yra nuožmiai ginčijamasi dėl VNC programinės įrangos dislokavimo. Didesnėje žemyninės Europos dalyje vyriausybės ir kompanijos griežtai draudžia naudojantis darbuotojų kompiuteriais prieiti prie bet kokios su darbu nesusijusios informacijos (nors tai nėra lengvai įgyvendinama). Elektroninio pašto tikrinimas griežtai laikomas neteisėtu.

Nusikaltimų atskleidimas visada buvo sunkiai suderinamas su piliečių laisvėmis, tačiau šių dviejų dalykų sambūvis tapo daug problemiškesnis nuo tada, kai išplito internetas, ir tai tęsis ateityje. Jei Vokietijoje policijos pareigūnas internetu anonimiškai seka įtariamąjį, jo internetiniam partneriui pareikalavus, teisiškai privalu pripažinti pareigūną įstatymo pažeidėju. Todėl ten labai sunku pritaikyti Britanijoje ir Jungtinėse Valstijose plačiai paplitusią praktiką, kai pareigūnai apsimeta nepilnamečiais berniukais ir mergaitėmis, norėdami įvilioti į pinkles pedofilus, jei įtaria, kad šie bando suvilioti vaikus internetu. VNC dislokavimas yra nepateisinamas politiniu požiūriu ir ribojamas svarbių duomenų apsaugos

įstatymų. Taigi Darrylas Leaningas su savo numylėtine turėjo elgtis labai rūpestingai.

Vieną 2008 m. vasario pradžios dieną Darrylo ekrane švystelėjo pranešimas, perspėjantis apie įtartiną programinę įrangą: „Neleistinos programos panaudojimas: *Messenger**." Darrylo sistemos sekė kelių tipų neleistinas programas. Žodis *Messenger* leido suprasti, kad kažkas bando įdiegti ar panaudoti panašų į „Skype"** bendravimo programų paketą. Per kelias minutes Darrylas atsekė, kad įspėjimas atsirado dėl vieno inžinieriaus chemiko, vieno iš svarbiausių GSA specialistų, veiksmų. Eidamas link įtarimą sukėlusio inžinieriaus darbo vietos, Darrylas nusprendė paprasčiausiai tiesiai jo paklausti, ar savo kompiuteryje jis paleido kokią nors naują bendravimo programą.

„O jis pasisuko į mane ir šaltakraujiškai pasakė: „Ne!" – kategoriškai tai paneigdamas. Taigi atsakiau: „O, gerai. Nors ir keista, nes aš ką tik gavau įspėjimą, kad šiame kompiuteryje veikia neleistina bendravimo programa."

Darrylas gūžtelėjo pečiais. Jo pernelyg nenustebino inžinieriaus atsakymas, kadangi saugumo sistemos yra jautrūs įtaisai, ir niekieno kito, o tik savo paties leidimu jis naudojo įvairias kruopščios peržiūros programas, kurios atrodė tarsi kokie įsibrovėliai į.jo paties prieš kenkėjus nukreiptą programinę įrangą. Šiaip ar taip, Darrylas nusprendė, kad net jei inžinierius ir naudojosi tokia programa, jis galbūt paprasčiausiai darbo laiku kalbėjosi su savo bičiuliais. Dabar jis bent jau žinos, kad elgėsi netinkamai, o jei vėl ja naudosis, Darrylas jį stebės. Taigi jis paprasčiausiai apie tai užmiršo.

Tačiau po dviejų savaičių nutiko tas pats. Šį kartą Darrylas nusprendė pažadinti galingąjį VNC žvėrį. Naršydamas po inžinieriaus

* Apsikeitimo greitosiomis žinutėmis programa (*messenger* – angl. pasiuntinys, kurjeris).

** Interneto telefonijos tinklas ir kompiuterinė programa, suteikianti galimybę skambinti į viso pasaulio šalis.

kompiuterį, jis pradėjo ieškoti bendravimo programos ir greitai nustatė, kad tai greitųjų pranešimų programa „Miranda“. Šiais laikais daug žmonių naudojasi greitosiomis žinutėmis, nes tai leidžia jiems tiesiogiai kalbėtis su draugais, mažuose tekstų langeliuose siunčiant jiems kelis žodžius ar sakinius. Daugeliu atvejų greitųjų žinučių programomis galima kalbėtis tik su tą pačią programinę įrangą turinčiais žmonėmis. „Mirandos“ pranašumas yra tas, kad norėdami bendrauti galite naudoti daugelį įvairių kalbėjimosi programų. Kai kuriems kompiuterių fanatikams tai ypač patinka.

Prieš paleisdamas į darbą VNC, Darrylas patikrino inžinieriaus standųjį diską, žiūrėdamas, ar neužtiks jame ko nors ypatingo, bet paieška pasirodė bevaisė. Buvo 12 val. 15 min., pats pietų metas. Kaip tik tinkamas laikas, pamanė Darrylas, trumpam paleisti VNC inžinieriaus kompiuteryje, norint kartą ir visiems laikams įsitikinti, ar jis iš tiesų naudojasi šia nelegalia programa.

„Miranda“ buvo visiški niekai, palyginti su tuo, ką Darrylas pamatė, kai VNC pradėjo tyrinėti darbuotojo kompiuterio paslaptis. Inžinierius buvo atidaręs dešimt tekstinių dokumentų vienu metu ir nežmonišku greičiu „bėgo“ per juos. Darrylas net išsižiojo iš nuostabos. Dar niekada jis nebuvo susidūręs su žmogumi, kuris sugebėtų taip greitai dirbti su dokumentais. Stebėdamas inžinieriaus ekraną, jis tespėjo įžiūrėti skaičių, simbolių ir žodžių miglą. Palengva jis suprato, kad inžinierius kopijuoja kažkokio dokumento dalis, kurias paskui perkelia į atskirą tekstinį failą.

Vis dar negalėdamas suprasti, nei kas vyksta, nei iš kur ateina visi šie dokumentai, Darrylas sugebėjo nustatyti tik tiek, kad tai nė trupučio nepanašu į kompanijos darbą. Dar didesnę painiavą sukėlė failo, į kurį jis kėlė tekstą, pavadinimas. Jis vadinosi „Sierra Leone“. Išeitų, kad inžinierius dirba prie naftos perdirbimo projekto Siera Leonėje. Darrylas su palengvėjimu atsiduso – galiausiai tai galėjo būti teisėtas darbas. Tik vėliau jam ėmė aiškėti, kodėl inžinierius

pasirinko šį pavadinimą. Jei kas nors eitų pro jo kompiuterį, jis paprasčiausiai „nuleistų" failą ir ant užduočių juostos ekrano apačioje praeinantysis matytų tik pavadinimą „Sierra Leone", – kaip tik prie šio projekto inžinierius ir dirbo.

Tai būtų suklaidinę ir Darrylą, jei VNC paskui nebūtų nustačiusi neregistruoto įrenginio F, o tai reiškė, kad inžinierius naudoja kažkokią nešiojamąją laikmeną. Darrylas pasiuntė VNC į paslaptingąjį įrenginį ir užsakė jai nukopijuoti dešimtis tūkstančių ten rastų dokumentų.

Vis dar nežinodamas, kaip elgtis toliau, ir nesugebėdamas nustatyti, kas, po galais, čia vyksta, Darrylas savo ištikimajai VNC nurodė dar sykį ištyrinėti įtartiną kompiuterį. Jis užprogramavo, kad VNC kas trisdešimt sekundžių darytų momentines inžinieriaus kompiuterio ekrano kopijas. Žiūrėti į kompiuterį tiesiogiai buvo labai sunku. Neįmanoma buvo nustatyti, ką iš tiesų reiškia šie duomenys. Tačiau kai Darrylas pamatė momentines ekrano kopijas – sustabdytus inžinieriaus veiklos vaizdus – jam toptelėjo gana aiški mintis apie tai, kas ten vyksta: tai buvo šimtų šimtai kreditinių kortelių numerių, banko sąskaitų, asmeninių duomenų, PIN kodų ir elektroninio pašto adresų. Tai visiškai nebuvo susiję su didėjančiais Siera Leonės naftos perdirbimo mastais.

Tada Darrylas išspausdino vieną itin tankiai užpildytą lapą su internetinio Amerikos banko duomenimis ir perdavė jį savo generaliniam direktoriui Maike'ui Smithui. Po kelių minučių Smithas paskambino Skantorpo policijai.

Kai detektyvas Dawsonas atvyko į „Grimley Smith" kompaniją, generalinis direktorius pateikė jam išspausdintą medžiagą. Ten buvo neįsivaizduojamos apimties duomenų rinkinys: informacija apie bankus, nekilnojamojo turto agentus, draudimo kompanijas, pramogų parkus, kino teatrus, labdaros organizacijas ir kitką, įskaitant ir kažką, kas buvo panašu į JAV karinę informaciją. Detek-

tyvui iš karto kilo įtarimas, kad susidūrė su kažkokia sukčiavimo forma, bet jis niekaip nesuprato, ką ta medžiaga galėtų reikšti ar nuo ko jam pradėti, norint patvirtinti šiuos įtarimus. Tai buvo sunkūs klausimai.

– Puiku, – pasakė Dawsonas, – pamėginkim pasikviesti jį pokalbio į kontorą, gerai?

„Grimley Smith“ vadovai nervingai žvelgė vieni į kitus.

– Ką tai reiškia? – paklausė Dawsonas.

– Jis yra stambi žuvis, – pasigirdo atsakymas, – ir, esu tikras, gali pasipriešinti.

– Na, mes išspręsime šią problemą, kai jos imsimės, – pasakė Dawsonas, demonstruodamas kuo didesnį autoritetą.

Bet kai aukštas, impozantiškas vyriškis įėjo į kontorą, Dawsonas pasijuto labiau šokiruotas nei supykęs. Kiek paniekinamai vyriškis paklausė detektyvo, kas jis toks ir ką čia veikia. Dawsonas išdėstė, kodėl buvo pakviestas į GSA, ir tiesiai paklausė, ką reiškia visi šie dokumentai. Netikėtai nerūpestingai vyras paaiškino, kad tai dalis ataskaitos, kurią jis sudarinėjo vienam iš kambaryje esančių vadovų. Akimirką stojo tyla, o tada vadovas maištingai pratarė:

– Ne, tai netiesa!

– Gerai, – pasakė Dawsonas, – ištieskite rankas, sere. – Ir linktelėjo savo kolegai: – Uždėkite jam antrankius!

Nė nebandydamas priešintis, ko taip bijojo vadovas, vyras visą laiką išliko gana ramus, nors ir šiek tiek suglumęs. Praėjus dviem valandoms po komandų ir kontrolės ataskaitos peržiūros, Dawsonas jau buvo suėmęs įtariamąjį ir pasodinęs jį į policijos kamerą. Bet dabar jis turėjo greitai paruošti bylą. Jei per tris dienas jis nesugebės rasti neginčijamų konspiracijos ar sukčiavimo įrodymų, turės paleisti šį žmogų, ir visas reikalas taip ir pasibaigs.

Dawsonas grįžo į „Grimley Smith“ su pareigūnu iš Moderniųjų technologijų atkūrimo skyriaus, ir juodu kartu su Darrylu Leaningu

kibo į darbą. Kaip Darrylas ir numatė, portatyvinės laikmenos buvo prigrūstos šimtų tūkstančių dokumentų, kurių dauguma buvo kimšte prikimšti kreditinių kortelių ir banko sąskaitų duomenų, nuskaitytų įsibrovus į kompiuterius. Bet ten taip pat buvo apsikeitimo elektroninėmis žinutėmis protokolai, iš kurių vienas buvo susijęs su interneto paslaugų sistemos „Yahoo!" naujienų grupe prozišku pavadinimu bankfraud@yahoogroups.com*. Šios grupės pranešimai ir įvairios žinutės labiau panėšėjo į universitetinio lygio paskaitas apie tai, kaip sukčiauti internete, nei į paprastas internetines konsultacijas.

Paskui Dawsonas nuvažiavo į gretimo Halio rajono *Plimsoll Way* gatvėje esantį butą, kur gyveno įtariamasis. Adrese nurodytas pastatas buvo panašus į doko rekonstrukcijos projekto vaisių, bet jau su pirmaisiais pastebimais nusidėvėjimo požymiais. Purvinos vandens paliktos dėmės teršė akmeninį fasadą, išėstą pro tinką prasimušusių rūdžių. Tai buvo tipiškas naujosios darbininkiškos Britanijos simbolis – švytintis ir ryškus iš išorės, bet nebegalintis ilgiau paslėpti surūdijusio vidaus, kuris veržiasi į paviršių.

Buto kambariai bylojo, kad čia gyvena viengungis. Tai anaiptol nebuvo kiaulidė, bet daiktai mėtėsi visur. „Trūksta moteriškos rankos", – pagalvojo Dawsonas. O tada miegamajame detektyvas atrado kai ką vertingo. Ant lovos gulėjo du nešiojamieji kompiuteriai, iš kurių vienas vis dar veikė. Ant jo pūpsojo didžiulė krūva dokumentų. Ten buvo ir nesuskaičiuojama daugybė „Western Union" kvitų, patvirtinančių pinigų pervedimus iš viso pasaulio: Naujosios Zelandijos, Meksikos, Jungtinių Arabų Emyratų, Ukrainos – iš įvairiausių šalių ir į jas.

Puiku, kad Dawsonas rado visus tuos failus ir dokumentus, bet, žinoma, tam, kad galėtų pareikšti kaltinimą, jam reikėjo ypatingo

* *Bank fraud* – bankiniai sukčiavimai. (Angl.)

nusikaltimo įrodymų. Beimant didžiulę šūsnį dokumentų, vienas lapas iškrito ir nupleveno ant grindų. Per tolesnius mėnesius Dawsonas dažnai pergalvodavo tą įžvalgos akimirką. Mat ant to lapo buvo vieno džentelmeno, gyvenančio kažkur Vakarų Jorkšyre, duomenys kartu su visais jo banko sąskaitų numeriais. Išstudijavęs juos Dawsonas suprato, kad tai gali būti gyvybiškai svarbūs nepaneigiami įrodymai, leisiantys pareikšti kaltinimą, nes ten buvo netgi slaptažodis. Jei tik galėtų įrodyti, kad šis žmogus niekada niekam nėra atskleidęs savo slaptažodžio, jis galėtų iškelti bylą. Štai kodėl detektyvas Dawsonas taip troško pasikalbėti su pastoriumi Andrew Arunu Johnu. Jei Johnas tai patvirtintų, tada Dawsonas galėtų apkaltinti įtariamąjį padarius ypatingą internetinio sukčiavimo nusikaltimą, ir labai tikėtina, kad teisėjas neišleistų jo už užstatą. Tada Dawsonas galėtų imtis Heraklio vertos užduoties – perplaukti per šį dokumentų vandenyną.

3
Misteris Haidas iš Lagoso

2003-iaisiais Adewale'as Taiwo gavo chemijos inžinerijos bakalauro laipsnį Lagoso universitete. Šis aukštas ir išvaizdus universiteto lektoriaus ir valstybės tarnautojos sūnus užaugo iškalbiu ir galvotu jaunuoliu su daug žadančia ateitimi pramonės ar akademinėje srityse. Pagal Nigerijos standartus, šeima buvo gana pasiturinti, be to, jie turėjo giminių Londone, galinčių padėti Adewale'ui tęsti mokslus Jungtinėje Karalystėje.

Tais pačiais metais, dar niekada nebuvęs Anglijoje, Adewale'as sukūrė savo antrininką Fredą Browną iš Oldamo Lankašyre, turintį tapti tikru kibernetinio pasaulio misteriu Haidu*. Būtent Fredas Brownas ir įkūrė „Yahoo" naujienų grupę apie bankinius sukčiavimus.

Netrukus Fredas Brownas jau platino skelbimus tokiose interneto svetainėse kaip „Hacker Magazine", „Alt 2600" arba „UK Finance":

> GALIMYBĖ: Verslo galimybė žmonėms, dirbantiems didžiuosiuose bankuose, arba tiems, kurie turi giminių ar draugų, dirbančių bankuose ir galinčių būti jų partneriais. Mus domina HSBC bankas, Škotijos karališkasis bankas,

* Misteris Haidas, blogasis daktaro Džekilio antrininkas, pramanytas veikėjas iš žymaus škotų rašytojo Roberto Louiso Stevensono kūrinio „Keistas daktaro Džekilio ir pono Haido atsitikimas" (1886), kuriame vaizdžiai aprašoma „susidvejinusios asmenybės" psichopatologija.

bet svarstytini ir kiti. Prašom atsakyti Fredui B. Brownui per „Yahoo“, „Icq“* arba „Safemail“.

Programišiams svarbu tai, kad šios programos yra „dinamiškos“, o tai reiškia, kad jos nepalieka pokalbio pėdsakų, nebent jei kas sąmoningai išsaugoja keitimosi žinutėmis protokolus. „Safemail“ yra šifruota elektroninių žinučių sistema, į kurią negalima įsilaužti. Nebent jei pavyktų įtikinti Izraelio teismą pareikalauti jūsų ieškomos informacijos liudijimui teisme, nes tai Tel Avivui priklausanti ir jo valdoma kompanija.

Atsakiusiesiems į Fredo Browno skelbimus būdavo siūloma prisijungti prie bankfraud@yahoogroups.com grupės, kurios tikslai ir moralė buvo aiškūs: „Ši grupė skirta žmonėms, kurie nori užsidirbti pinigų, bet nenori dirbti legaliai ir yra pasirengę laužyti taisykles. Šioje grupėje jūs išmoksite apgauti bankus ir pavogti tapatybės duomenis.“ Fredas taip atvirai galėjo reklamuoti savo kėslus internete, nes apgavystėmis paremta veikla čia jau buvo paplitusi. Praėjo keleri metai, kol jį pastebėjo teisėsaugos institucijos, ir tai atsitiko tik todėl, kad galiausiai jis padarė jam nebūdingą kvailą klaidą.

Fredo reklamos buvo sukurtos taip, kad priviliotų lengvatikius tradiciniu būdu – galimybe dirbti savo buvimo vietoje. Jei galite įtikinti banko darbuotoją nuvogti kliento duomenis ir juos perduoti, jums nereikia vargti įsilaužiant į sistemą, kad išgautumėte sąskaitų ar kreditinių kortelių duomenis. Internetiniai sukčiai deda daug pastangų, mėgindami rasti nepatenkintų ar vargstančių bankų darbuotojų, nes turėdami patikimą banke dirbantį žmogų gali smarkiai padidinti savo uždarbį. Gavęs sąskaitos duomenis, nusikaltėlis gali

* Trumpųjų žinučių programa „Icq“ (pavadinimas kilęs iš angliškų žodžių *I seek you* (aš ieškau tavęs) ir senesnis jos variantas IRC (angl. *Internet Relay Chat* – pokalbiai, perduodami internetu) yra labai mėgstamos programišių (angl. *hacker*) ir įsilaužėlių (angl. *cracker*).

laisvai įeiti į sąskaitą internetu, tarsi ši būtų jo paties, o paskui pervesti grynuosius į savo pasirinktą sąskaitą. Išskyrus tuos atvejus, kai įsilaužėliui nedelsiant reikalinga didelė pinigų suma, mėgstamiausias vagišių metodas – ilgą laiką imti mažas sumas taip, kad nepastebėtų nei bankas, nei jo klientas.

Tačiau Fredas taip pat kūrė ir kai kuriuos pažangesnius sukčiavimo metodus. Jis sugebėjo įeiti į bankinę sistemą giliau ir ten galėjo užsiimti tokiais darbeliais kaip, pavyzdžiui, sąskaitos kredito limito padidinimas. Regis, jis išmanė, kaip pakeisti pavardes ir adresus ir, be abejo, kaip išgauti slaptažodžius.

Sukurdamas pamatus šiai veiklai daug anksčiau, nei atvyko į Jungtinę Karalystę, Fredas pademonstravo savo sisteminį požiūrį į verslą. Jis buvo vertinamas, nebuvo socialiai nesaugus ir negaišo daug laiko, žaisdamas kompiuterinius žaidimus. Fredas Brownas (dar žinomas kaip Freddy Brownas, Fredas B. Brownas, Freddy B, FredB ir Freddybb) internetą laikė paprasta ir lengva priemone, leidžiančia apgaulės būdu išvilioti dideles pinigų sumas iš nesuskaičiuojamos daugybės žmonių.

Bet prieš išleisdamas Fredą į internetą jo Džekilis – Adewale'as Taiwo – turėjo kitų reikalų: vienus metus jis studijavo chemijos inžinerijos magistrantūroje Mančesterio universitete, į kurį atvyko 2005 m. spalį. Mėnesiu anksčiau, nei jam buvo suteiktas magistro laipsnis (2006 m. gegužę), jis atidarė sąskaitą Londono aukso biržoje LGE (angl. *London Gold Exchange*), į kurią galėjo pervedinėti pinigus iš bet kurio didžiojo banko.

LGE perka auksą už jūsų įdėtus pinigus ir suteikia jums „skaitmeninės valiutos" kreditą. Londono aukso birža, nors ir neteisingai taip vadinama, nes jos būstinė yra Belize, o auksas saugomas Šveicarijoje, – viena iš kelių praeito amžiaus paskutiniame dešimtmetyje išsiplėtusių įstaigų, labai pamėgta sukčių ir pinigų plovėjų. Permetęs pinigus į Londono aukso biržą, Fredas Brownas paskui

juos persiųsdavo į savo sąskaitą panašioje institucijoje „E-Gold"*, o iš ten per „Western Union" išskirstydavo valiutą po visą pasaulį, taip ją išplaudavo arba panaudodavo atsiskaityti su savo bendrininkais.

Kaip ir visose veiklos srityse, jis ir čia pasirodė esąs kruopštus ir produktyvus: puikus studentas ir gudrus nusikaltėlis. „Grimley Smith" pastvėrė jį kaip perspektyvų specialistą netrukus po to, kai Mančesterio universitetas suteikė jam magistro laipsnį. Tuo pat metu internetinių sukčių brolija priėmė jį į savo gretas kaip rimtą žaidėją.

Adewale'as Taiwo buvo talentingas chemijos inžinierius. Dar nesulaukęs trisdešimties, jis buvo laikomas vienu iš aukštai kilsiančių „Grimley Smith" kompanijos darbuotojų ir netrukus darbo reikalais jau keliavo į tokias tolimas šalis kaip Kinija ir Venesuela. Jis gerai rengėsi, bet savo apranga niekada nesistengė išsiskirti, o jo BMW atitiko atlyginimą ir gyvenimo būdą. Abu savo gyvenimus jis vertino labai rimtai ir, be abejo, jo legalus darbas buvo patikima priedanga, sauganti pogrindinę veiklą. Gerbiama ir klestinti energetikos sektoriaus kompanija yra viena iš paskiausių vietų, kur būtų galima ieškoti stambaus kibernetinio nusikaltėlio, juo labiau tarp darbščių aukštos kvalifikacijos firmos inžinierių.

Kai detektyvas seržantas Chrisas Dawsonas pradėjo domėtis Fredo Browno sukčiavimo mastais, buvo pritrenktas. Net ir gerokai sumažinęs duomenų kiekį, jis vis dar turėjo peržiūrėti apie 34 000 failų, o kai kurie iš jų buvo nuo 100 iki 150 puslapių apimties. Jau pradžioje seržantas pastebėjo vieną 100 puslapių failą, prigrūstą amerikietiškų kreditinių kortelių numerių su apsauginiais kodais ir visais reikalingais slaptažodžiais.

* E-Gold – skaitmeninė aukso valiuta, kurią jos turėtojai galėjo nedelsdami pervesti kitiems naudotojams iki 2009 m., kai šie pervedimai buvo uždrausti.

Detektyvas Dawsonas buvo žmogžudysčių skyriaus pareigūnas – niekas Hambersaide* niekada nebuvo dirbęs prie aukštos klasės internetinių sukčiavimų, taigi juodu su kolega turėjo atlikti ir savo kasdienius darbus. Jis paprasčiausiai neturėjo supratimo, nuo ko pradėti. Kartu su failais ten buvo ir programinė įranga prietaisui MSR206. Šis įrenginys yra galbūt svarbiausias ginklas sukčiautojų kreditinėmis kortelėmis, kurie vadinami bendru terminu „karderiai"**, arsenale. Šiuo prietaisu jie gali „klonuoti" kreditinę kortelę: nukopijuoti visą informaciją nuo kitoje pusėje esančios magnetinės juostelės ir perkelti ją ant švaraus balto plastiko gabalėlio su tuščia magnetine juostele. MSR206 yra asmeninė pinigų kalykla.

Failuose Dawsonas taip pat rado klaviatūros sekimo programų (angl. *keyloggers*) trojanų. Nusikaltėliui programišiui tai tas pats, kas seifų plėšikui laužtuvas. Ankstyvieji virusai labai skyrėsi nuo klaviatūros sekimo programų. Kai praeito šimtmečio paskutiniame dešimtmetyje dideliais kiekiais pradėjo cirkuliuoti pirmieji virusai, juos kūrė paaugliai ir studentai, norintys pademonstruoti savo anarchiško programavimo meistriškumą. Pikčiausia, kad jie siekė sugadinti kuo daugiau kompiuterių visame pasaulyje.

Kai jūsų kompiuteris užkrečiamas, jis gali elgtis bet kuriuo iš daugelio būdų: jo darbas gali sulėtėti; jei jūs išsikviesite vieną programą, tarkim „Microsoft Word", vietoj jos gali atsidaryti interneto naršyklė; jūsų kompiuteris gali automatiškai išsijungti; o blogiausia – gali būti sugadinti jūsų failai ir duomenys. Teko girdėti pasakojimų apie autorius, kurie dėl kažkokio žalingo viruso prarado ištisus rankraščius, ir apie statistikos darbuotojus, kurių akyse mėnesių mėnesius įvedinėtus duomenis prarijo bjaurus skaitmeninis kirminas.

* Šiaurės Anglijos grafystė.

** Karderis (angl. *carder*) – sukčius, naudojantis pavogtų kreditinių kortelių duomenis apgaulingiems internetiniams sandėriams atlikti; kardingas (angl. *carding*) – apgaulingų internetinių sandėrių atlikimas, naudojantis vogtais duomenimis. Pavadinimai kilę iš angl. žodžio *card* – kortelė.

Tačiau, perėjus į naują tūkstantmetį, programišiai, įsilaužėliai ir kiti nusikaltėliai pradėjo suprasti, kad virusai, trojanai ir kirminai* gali būti panaudoti pelningesniems tikslams. Atsirado klaviatūros sekimo programa, kuri itin greitai dauginosi internete. Sykį įsisukusi į jūsų kompiuterį, ši maža nenaudėlė seka kiekvieną jūsų klaviatūros klavišo spustelėjimą. Taigi kai jūs įvedate www.hsbc.co.uk į savo interneto naršyklę, ji persiunčia šią informaciją jos kūrėjui arba turėtojui, kuris gali būti bet kurioje pasaulio vietoje. Jei tuomet jūs įvestumėte savo slaptažodį, tarkim, „Robinhudas", viruso vadovas Naujajame Džersyje, Rostoke, Lilongvėje ar bet kokios išgalvotos Ruritanijos gilumoje jį užregistruotų. Puiku! *Mi cuenta bancaria es su cuenta bancaria!*"

Vis dėlto tūkstančių kreditinių kortelių duomenų ir bankinių sąskaitų numerių saugojimas kompiuteryje dar nėra nusikaltimas, tas pats pasakytina ir apie klaviatūros sekimo virusą. Tai gali būti rimtas nusikalstamos veiklos požymis, bet jo nepakanka bylai iškelti. Naršydamas begalinius failus, Dawsonas su savo kolega turėjo išnarplioti šimtus susipainiojusių gijų.

Rankiniu būdu suvedę keletą tūkstančių sąskaitų rekvizitų į duomenų apdorojimo sistemos „Excel" lentelę, policininkai nusprendė kreiptis į bankus. Kai kam gali atrodyti, kad tai itin išmintinga, nes, šiaip ar taip, būtent į bankų saugumo sistemas Fredas Brownas taip sėkmingai įsilaužda vo.

Kur tau!

* Paprasčiausias, nors ir nepakankamai išreikštas skirtumas tarp virusų, kirminų ir trojanų, bendru vardu vadinamų „kenkėjiškomis programomis", susijęs su jų perdavimo metodu – virusai plinta per užkrėstus elektroninių žinučių priedus, trojanai – per atsisiųstą informaciją, o kirminai sugeba savaime daugintis užkrėstame kompiuteryje ir paskui, naudodamiesi to kompiuterio bendravimo programomis, pasklisti po kitus kompiuterius. Bet iš esmės visi jie yra kenksmingi kompiuteriams. (Aut. past.)

** Tavo banko sąskaita yra mano banko sąskaita! (Isp.)

Daugelis Dawsono užklausų atsimušė kaip žirniai į sieną, nes bankai paprasčiausiai net nesivargino atsakyti į jo prašymus. Per visą tyrimą detektyvą spaudė laikas, jis daug jo iššvaistė bergždžiai stengdamasis įtikinti bankus bendradarbiauti.

Daugumos bankų požiūris į kibernetinius nusikaltimus yra nevienareikšmis. Rašant šią knygą man paskambino vienas džentelmenas iš mano banko „NatWest" ir paklausė, ar pastaruoju metu aš nepirkau ko nors iš Bulgarijos sostinės Sofijos juvelyrų. Dar daugiau, jis pasiteiravo, ar aš sumokėjau 4 000 frankų už Šveicarijos telekomo sąskaitą. Pasakiau, kad nieko panašaus nedariau. Tada man buvo pranešta, kad buvo pasikėsinta į mano „NatWest" banko „Visa" kortelę ir kad aš turėsiu pasiimti naują kortelę, bet galiu jaustis saugus, nes „NatWest" anuliavo 3 000 svarų operaciją, atliktą apgaulės būdu panaudojus mano kortelės duomenis. Kaip ir bet kuris kitas, kuriam teko tai patirti, aš pajutau didžiulį palengvėjimą, kai bankas dar sykį maloniai mane patikino, kad man už tai mokėti neteks.

Bet kas iš tiesų už tai sumoka? Bankai? Ne, jie apdrausti nuo tokių nuostolių. Draudimo kompanijos? Ne, nes jos nustato tokio dydžio draudimo įmokas, kurios užtikrina, kad kompanijos nepatirs materialinės žalos. Tai gal vis dėlto bankai, nes jie moka draudimo įmokas? Taip. Bet jie susigrąžina pinigus, apdėdami papildomais mokesčiais visus savo klientus. Iš esmės už bankines apgavystes sumoka visi banko klientai.

Nenuostabu, kad bankai nelinkę šito plačiai viešinti. Jie taip pat nenori, kad visuomenė žinotų, kaip dažnai kibernetiniai nusikaltėliai kėsinasi į jų sistemas. Jie neteikia žurnalistams jokios informacijos apie kibernetines atakas, užgriūvančias juos kiekvieną dieną. Tai suprantama. Mažiau pateisinamas jų dažnas nenoras bendradarbiauti su policija, nes informacija gali būti atskleista viešame teismo posėdyje. Bijodami prarasti pranašumą prieš konkurentus ir todėl atsisakydami pripažinti, kad jų klientai tampa kibernetinių nusi-

kaltimų aukomis, bankai netiesiogiai padeda nusikaltėliams dirbti savo darbą.

Žinoma, bankai turi problemą: jų klientai yra pažeidžiamiausia tinklinės finansinės sistemos dalis. Šiais laikais net ir aukščiausios klasės programišiams įsilaužti į pagrindinių mažmeninių ir investicinių bankų kompiuterių sistemas yra sunkus uždavinys. Bet patekti į daugumos klientų kompiuterius ir stebėti, kaip jie prieina prie savo sąskaitų ir, be abejo, atlieka pinigines operacijas, bet kuriam gabiam programišiui (jam ar jai, nors paprastai tai būna jis) yra tik vaikų žaidimas. Kaip patobulinti klientų naudojimosi internetu įpročius, kai internetinė bankininkystė (kaip ir daugelis kitų mūsų internetinių užsiėmimų) mus labiausiai traukia savo patogumu? Paprastai žmones atgraso sudėtingos saugumo procedūros, kurias reikia atlikti, norint prieiti prie savo sąskaitų, nes tai labai vargina.

Bankai linkę nutylėti apgavysčių mastą iš dalies dėl konkurencinių priežasčių, iš dalies dėl to, kad nenori, jog jų klientai pareikalautų sugrįžti prie senųjų metodų. Elektroninė bankininkystė jiems sutaupo milžiniškas pinigų sumas, nes klientai patys atlieka tas užduotis, kurias anksčiau atlikdavo bankų filialų darbuotojai. Jei mes visi atsisakytume tvarkyti savo finansus internetu, bankai būtų priversti atkurti didžiulį filialų tinklą, per kurį mus anksčiau aptarnaudavo. Tai kainuotų didžiulius pinigus, o kaip mes dabar jau žinome, bankai išleido viską, ką turėjo, ir dar šimtus milijardų mokesčių mokėtojų pinigų, suteikdami paskolas didžiausioms rizikingoms avantiūroms ir išsimokėdami sau nepadoriai išpūstus dividendus.

Taigi detektyvas Dawsonas buvo įpareigotas išspręsti sudėtingą galvosūkį, turėdamas labai ribotą bankinės bendrijos paramą. Tačiau jam pravertė tai, kad Fredas Brownas, kurdamas savo apgavysčių tinklą, padarė porą reikšmingų klaidų: nors jo bankinių sukčiavimų grupė „bankfraud@yahoogroups.com“ buvo įregistruota Amerikoje,

jai buvo priskirtas elektroninio pašto adresas yahoo.co.uk. Kadangi tai buvo Britanijos domeno pavadinimas, Dawsonas galėjo nedelsdamas perduoti teismui reikalingą medžiagą iš „Yahoo". Sunkiau sekėsi su „Safemail" pranešimais. Jam teko prašyti Britanijos teismo kreiptis į Izraelio teismą su prašymu, kad „Safemail" leistų prieiti prie Fredo Browno šifruotos sąskaitos. Tai užtruko keletą mėnesių, o per visą tą laiką teismai jį spaudė atskleisti parodymus advokatams ir pagreitinti įvykių eigą.

Dawsono viršininkai buvo nepatenkinti. Jis jautė didėjantį spaudimą. Nė viena jo tiriamo nusikaltimo auka nebuvo iš Hambersaido – kreditinių kortelių turėtojai buvo išsibarstę po visą pasaulį. Vienas iš jų – pastorius Johnas – gyveno kaimyniniame Vakarų Jorkšyre, bet kas iš to? Ne sykį Dawsonas girdėjo savo valdžios perspėjimą: „Aš negaliu leisti, kad vienas iš mano geriausių Žmogžudysčių skyriaus pareigūnų dirbtų prie sukčiavimo bylos, neturinčios nieko bendro su šiuo regionu!" Tačiau ši detektyvinė istorija kažkuo jį vis dėlto traukė. Jis nesiruošė pasiduoti, taigi, norėdamas nuraminti vyresnybę, pradėjo dirbti laisvalaikiu ir kartais iki vėlumos įnikdavo į skaičius, šokinėjančius jam prieš akis.

Apimtas nevilties, kad Adewale'o Taiwo bylos nagrinėjimas suryja marias laiko, Dawsonas paprašė regioninio žvalgybos padalinio pagalbos. Jie niekuo nepadėjo, tačiau patarė kreiptis į Londono miesto policijos Moderniųjų technologijų skyrių ir paklausti, ar jie neturi informacijos, galinčios jam praversti. Ne, atėjo atsakymas, bet kodėl jums nesikreipus į Sunkių organizuotų nusikaltimų agentūrą SOCA?

Galiausiai Dawsonas paskambino į SOCA slaptųjų operacijų būstinę Londone, kažkuo primenančią Leno Deightono romanus *IPCRESS failas* (*The IPCRESS File*) arba *Laidotuvės Berlyne* (*Funeral in Berlin*): žalvario plokštelės su fiktyvios kompanijos pavadinimu, ir visi apsimeta, jog nedirba tarnyboje, kurią Tony Blairas

apibūdino kaip Britanijos atkirtį FTB (tuo labai suerzindamas jos pareigūnus).

Dawsonas paprašė pagalbos tiriant sudėtingą sukčiavimo bylą, į kurią įsipainiojęs paslaptingas vyriškis, vadinamas Fredu Brownu, ir išgirdo trumpą ir atžarų didžiųjų sostinės vyrukų atsakymą:

– Ką tu žinai apie Freddie Browną?

Šiaip ar taip, tu esi tik menkas varguolis iš Hambersaido, – buvo galima suprasti iš kalbančiojo balso tono.

– Nieko, – atsakė detektyvas Dawsonas, – išskyrus tai, kad čia, Skantorpe, aš turiu jį sulaikęs kardomajam kalinimui.

Linijos gale stojo tyla.

– Ar kada nors esate ką nors girdėję apie „DarkMarket“, detektyve seržante Dawsonai? – paklausė tas pats balsas.

– Ne, niekada. O kodėl klausiate?

Atrodo, kad Dawsonas pagavo didesnę žuvį, nei pats įsivaizdavo.

Bet ši žinia nė kiek ne mažiau nustebino ir SOCA. Jau kelerius metus jie sekė Freddybb, tačiau „DarkMarket“ tyrimas po kelių areštų praeitą vasarą kuriam laikui buvo aprimęs. Jie net neįsivaizdavo, kad policininkas iš Skantorpo galėtų jį atgaivinti. Tačiau nuo tada, kai grupė kibernetinių vagišių iš Ukrainos 2001 m. įkūrė pirmąją pasaulinę internetinių nusikaltimų svetainę, didžiausias Britanijos internetinių nusikaltimų tyrimų padalinys, be visų kitų, suprato dar vieną tiesą – visada tikėkis neįtikėtino.

II dalis

4
Odesos failai

Odesa, Ukraina, 2002 m. birželis

Jie atvyko iš tolimo Sankt Peterburgo šiaurėje ir iš Latvijos prie Baltijos jūros. Vienas delegatas atkeliavo iš Baltarusijos – tarsi kokio 1990 m. įkurto gyvojo paminklo komunizmui, kur dar nemažai galios turėjo rusai. O šeimininkė Ukraina sukvietė delegatus tiek iš vakaruose esančio Ternopolio ir sostinės Kijevo, tiek iš Charkovo šiaurėje ir Donecko rytuose.

Pirmoji pasaulinė karderių konferencija FWCC (angl. *First Worldwide Carders' Conference*) buvo iš tiesų tarptautinė. Kai kurie dalyviai atvyko iš Vakarų Europos, o kiti atskrido iš tokių tolimų vietų kaip Persų įlanka, Kanada ir Pietų Amerika. FWCC spaudos pranešimuose apgailestavo, kad dėl kelionės sunkumų negalėjo atvykti delegatai iš Australijos ir Pietryčių Azijos.

Iš 400 gautų pareiškimų organizatoriai atrinko apie tris tuzinus delegatų. Tie laimingieji, kurių kandidatūroms buvo pritarta, suprato, kad jau vien pakvietimas smarkiai pakels jų autoritetą nuožmiai hierarchijai pavaldžiame internetinių nusikaltėlių pasaulyje.

Kad jų pėdsakais neatsektų policija, organizatoriai iš pradžių paskelbė, kad ruošia renginį keliose prabangiose jachtose,

prisišvartavusiose Juodosios jūros pakrantėje Turkijoje. Bet tai buvo paprasčiausias melas. O ir kur kitur būtų galima surengti pirmąją kibernetinių sukčių konferenciją, jei ne Odesoje – legendiniame Ukrainos sukčių mieste?

Naudodamiesi savo gerai išbandytais metodais, tiek caras, tiek Stalinas ir Hitleris bandė sutramdyti šį laukinį žvėrį, bet nė vienam iš jų nepavyko sutriuškinti ilgiausiai išsilaikiusios Rytų Europos nusikaltėlių brolijos. „Nesuprantant Odesos gangsterių ir jų gyvenimo, – rašė vienas metraštininkas apie savo gimtąjį miestą, – neįmanoma suprasti miesto istorijos."

Nuožmus laukinis gangsterių kapitalizmas, iškilęs žlugus komunizmui praeito amžiaus paskutiniame dešimtmetyje, užgriuvo didžiąją dalį Rytų Europos ir sukėlė tikrą šoką. Bet Odesa žinojo, kas jos laukia. Odesos gyventojai neturėjo kito pasirinkimo, kaip tik drąsiai pasitikti naują erą – ir, reikia pripažinti, jie tai padarė ganėtinai audringai. Raudonos žvaigždės per naktį buvo pakeistos raudonais žibintais. Bulvare Primorskij kaip piktžolių pridygo tamsių kazino, o po 1989 m., visai netrukus, restoranuose ir saunose vyko apsirijėliškos puotos ir liejosi kraujas.

Toliau nuo centro, gyvenamųjų namų rajonuose, valiutos pakaitalu tapo narkotikai. Pinigų neturintys jaunuoliai pamėgo „boltuškas" – namų darbo amfetamino mišinį, nuo kurio daugelis jų liko fiziškai arba protiškai neįgalūs arba mirė.

Banditai ir jų klanai iš tokių tolimų vietų kaip Čečėnija ir Maskva kovėsi su vietiniais robinais hudais dėl valdžios mieste – nors Odesa teoriškai buvo naujos nepriklausomos Ukrainos dalis, ji buvo rusakalbė ir, kas dar svarbiau, vienintelis neužšąlantis uostas, pajėgus eksportuoti Rusijos dujas ir naftą.

Hiperinfliacija ir nacionalizmas nuvertino rublį, karbovancus, grivinas ir visa kita, ką valdžia vienu ar kitu metu buvo paskelbusi „realiais" pinigais. Tiktai jankių doleriai suteikdavo bent kiek tikro stabilumo.

Praeito amžiaus paskutiniame dešimtmetyje daugumai paprastų Odesos žmonių svarbiausi buvo du dalykai: išgyvenimas ir doleriai. Niekam nerūpėjo, kaip jums pavyksta išgyventi ar iš kur gaunate pinigų. Iš tiesų žmonės vertino tuos, kurie sugeba ir viena, ir kita, nors greitas praturtėjimas neužtikrino ilgo gyvenimo.

Ir kas gi šioje atmosferoje būtų galėjęs kaltinti trylikametį Dimitrijų Golubovą už tai, kad jis pardavinėja automobilių registracijos dokumentus ir vairuotojų teises su padirbtais savivaldybės Transporto skyriaus viršininko parašais? Jei verslininkai noriai už tai mokėjo, argi tai nereiškia, kad tokia prekyba buvo reikalinga?

Štai tokia buvo Odesa. Bet jaunasis Dimitrijus pasižymėjo viena savybe, kuri neleido jam atsidurti tradiciniame miesto gangsterių pasaulyje su reketininkais, viešnamiais, nafta ir ikrais. Užuot nešiojęsis peilį, jis ilgam pranykdavo tamsiuose prirūkytuose rūsiuose, kur nuo tokių kompiuterinių žaidimų kaip „Gatvės kovotojas", „Pakmanas", „Rusų klasikinis" ar „Tetris" greitai skystėjo paauglių smegenys. Šioje pogrindinėje kultūroje vienintelę šviesą skleidė švelnių spalvų neoninis apšvietimas ir mirgantys kompiuterių ekranai. Cigaretės ir „Coca-Cola" buvo taip plačiai paplitę, kad atrodė kaip vienintelis pagal kažkokią senovinę keistuolių išmintį toleruojamas košerinis maistas.

Dimitrijus mėgo žaidimus kaip ir visi kiti, nors sėdint patogiose Odesos interneto kavinėse jam labiau patiko tyrinėti pasaulį. Bet jaunasis Golubovas ne tik mėgo naršyti po tolimų kraštų svetaines, jam rūpėjo įsiskverbti į jas ir patyrinėti giliau.

1999-aisiais, kai jam sukako šešiolika, buvo užblokuotas „Visa" ir „MasterCard" kortelių naudojimas buvusioje Sovietų Sąjungos teritorijoje įregistruotose interneto svetainėse. Kai Rusijos interneto kompanijos pateikė sąskaitas šiedviem kredito milžinams, jos paprasčiausiai buvo ignoruotos. Bet Golubovas su savo jaunaisiais bičiuliais greitai suprato, kad jei kokiu nors

būdu pavyktų išgauti kreditinėje kortelėje esančią informaciją ir ją atgaminti, tuos duomenis būtų galima panaudoti gryniesiems pinigams paimti iš bankomatų arba perkant prekes internetu, o paskui persiųsti jas į kur nors kitoje pasaulio vietoje esančią trečią šalį. Vienas variantas buvo nukopijuoti šią informaciją iš pačios fiziškai egzistuojančios kreditinės kortelės, nors iš pradžių tai reiškė daug pastangų reikalaujančią ir todėl nepageidautiną tradicinę vagystę. Daug geriau buvo (ir lig šiol yra) paprasčiausiai ištraukti informaciją iš aukso kasyklų – kompanijų duomenų bankų!

Nors kai kurios Amerikos svetainės nepristatinėjo prekių į buvusią Sovietų Sąjungą, jos patenkintos siuntė jas į tokias vietas kaip Jungtiniai Arabų Emyratai ir Kipras – dvi šalis, kurias greitai labai pamėgo pinigingasis Rusijos elitas. Tai buvo vieni iš pirmųjų tikrai globalinių nusikaltimų. Ukrainos rusai vogdavo pinigus iš Amerikos kompanijų, o sumokėdavo Dubajuje – ir visas sandėris neužtrukdavo ilgiau nei dešimt minučių!

Kitas didelis perversmas, kuris suformavo naują profesiją – „kardingą", buvo vadinamųjų nelegalių skaitytuvų (angl. *skimmer*) sukūrimas. Tai prietaisai, nuskaitantys ir išsaugantys kreditinės kortelės magnetinėje juostelėje esančią informaciją. Jų būna kelių formų ir dydžių. Kai kurie yra maži kvadratiniai, jie gali būti pritvirtinami prie bankomatų taip, kad tuo metu, kai nuskaitoma kliento kortelė, ją taip pat nuskaito ir šis prietaisas. Kiti visai nesiskiria nuo prekybos vietose esančių skaitytuvų, kuriais naudojasi padavėjai ar degalinių kasininkai, kai klientas moka kortele. Tiek prie bankomato, tiek prie prekybos vietos skaitytuvo kažkur turi būti pritaisyta mažytė slapta kamera, įrašanti kliento įvedamą PIN kodą (įsidėmėkite: įvesdami PIN kodą, *visada* uždenkite klaviatūrą).

Nedorais tikslais naudojami kortelių skaitytuvai veikia lygiai taip pat kaip ir tie, kurių galima nusipirkti. Kartais nusikaltėliai įsigyja prekybai pagamintų skaitytuvų, kitais atvejais jie yra namų

darbo. Šių prietaisų panaudojimas kortelėms nuskaityti prilygsta Jameso Watto garo variklio išradimui pramoninės revoliucijos pradžioje. Per dešimtmetį nuo jų pasirodymo dauguma sukčiavimams panaudotų kreditinių kortelių numerių ir PIN kodų visame pasaulyje buvo nuskaityta būtent jais.

Būdamas talentingas programišius, Dimitrijus greitai suprato, kad vos užgimusios Jungtinių Valstijų elektroninės prekybos apsaugos sistemos yra primityvios ir į jas lengva įsilaužti. Visiškai nežinoma, kaip jam sekėsi iš pradžių. Dimai patiko skleisti gandus, kad jis sukaupė milijoną dolerių auksu dar prieš švęsdamas savo septynioliktąjį gimtadienį. Tačiau nepamirškime, kad melas yra labiausiai paplitusi internetinė valiuta. Kai kurie jo kibernetiniai draugužiai pasakoja visai kitokią istoriją.

„Jis buvo godus, nesąžiningas ir jį visada traukė kriminalinė aplinka, – rašė kitas Odesos programišius, – tačiau sėkmingo milijonieriaus įvaizdis toli gražu neatitiko tikrovės."

Tuomet Dimitrijus pranyko kartu su savo piktinančiomis pinigų „darymo" schemomis. Po kelių mėnesių tarsi drugelis iš lėliukės jis pasirodė nauju anoniminiu vardu Skriptas (*Script*). Tai buvo nepaprastai sumanus personažas, skraidantis tarp dviejų naujų interneto svetainių: „carder.org" ir „carder.ru". Jos buvo šiek tiek daugiau nei diskusijų forumai. Šiose svetainėse rusų programišiai aptarinėjo, kaip techniškai būtų galima prieiti prie nesuskaičiuojamų milijonų dolerių, svarų, jenų ir eurų, „užrakintų" kreditinėse kortelėse. Vienas iš pirmųjų šių svetainių narių prisiminė, kad visa ši veikla buvo „padrika, nestabili" ir galiausiai „nepelninga".

Tačiau Skriptas mąstė ilgai ir rimtai. Jei egzistuoja visokių rūšių prekybai skirtos svetainės, kodėl nesukūrus tokios, kur būtų prekiaujama vogtais kreditinių kortelių ir banko sąskaitų numeriais ir kitais vertingais duomenimis? Jis turėjo įtikinamą motyvaciją sukurti internete šį paslaptingą personažą, kadangi pats jau buvo

pradėjęs dideliais kiekiais kaupti tokią informaciją, tačiau neturėjo nei laiko, nei galimybių ja pasinaudoti. Jis norėjo visus tuos skaičius paversti valiuta. Norėjo juos parduoti.

Laikas tam buvo labai palankus. Per penkerius ankstesnius metus komercinė veikla internete nepaprastai išaugo. To niekas rimtai nesitikėjo, nes interneto kūrėjai įsivaizdavo jį kaip priemonę bendravimui pagerinti ir pagreitinti, kaip vietą, kur būtų galima apsikeisti idėjomis ar tiesiog paplepėti.

Internetinėje erdvėje iškilo „Amazon", „eBay", „lastminute.com"* ir kiti kibernetinio pasaulio iniciatyvų pradininkai. Jų sėkmė neliko nepastebėta. Tūkstančių tūkstančiai miklino rankas, kurdami savo interneto svetaines. Tai buvo vienas iš tokių istorinių momentų, kai žmonių godumas atitinka jų fantaziją. Toks pasitaiko gal tik kartą kiekvienoje kartoje. Netrukus bankai ir rizikos kapitalas įtikėjo, kad elektroninė prekyba gali užtikrinti greitą praturtėjimą. Jie pradėjo investuoti pinigus į šias kompanijas, kurių didžioji dalis iš esmės buvo beverčiai subjektai, nors jų kapitalas siekė milijonus, jei ne dešimtis milijonų. Buvo išpūstas pirmasis svarbus globalizacijos amžiaus burbulas ir, kaip pridera, tas burbulas buvo iš moderniųjų technologijų srities.

Tačiau nors dauguma internetinės prekybos kompanijų iš tiesų buvo komerciniai Potiomkino kaimai**, realiame pasaulyje jau gerai įsitvirtinusios firmos suprato, kad jos gali įgyti išskirtinių pranašumų, dalį savo verslo perkeldamos į internetą.

Bankai šiuo atžvilgiu greitai apsisprendė, nes, kaip jau buvo minėta, suprato, kad jei sugebėtų įtikinti savo klientus atlikti mokėjimus ir tvarkyti banko sąskaitas internetu, už šį darbą nereikėtų mokėti darbuotojams. Jie buvo beveik tikri, kad tiems klientams, kurie

* Internetinės prekybos ir kelionių rezervavimo svetainės.

** Butaforinis kaimas; šis posakis reiškia apgavystę, norint prieš ką nors geriau pasirodyti.

įpratę naudotis internetu, labiau patiks patiems kruopščiai tvarkyti savo finansus, o tai ir leido daryti internetinė bankininkystė.

Tuo metu visatos valdovai – nauja finansų magnatų klasė – nusimetė pančius, kurie praeityje varžė jų spekuliatyvią veiklą išvestinių finansinių priemonių rinkose. Iš esmės leidimą spekuliuoti jiems davė Vašingtono ir Londono politikai (internetinės prekybos bumas buvo puikus to pavyzdys) ir, iki milžiniškų aukštumų pakilus mažą vertę turinčio turto kainoms, pinigai buvo skolinami pagal tariamai išaugusią to turto vertę. Dešimtį metų Vakarų pasaulis maudėsi pigiuose kredituose. Imperijos amžių ir Kapitalo amžių pakeitė Plastikinių kreditinių kortelių amžius.

Asmeninės kreditinių kortelių skolos keturiose daugiausia šių kortelių turėtojų turinčiose šalyse – JAV, Jungtinėje Karalystėje, Japonijoje ir Kanadoje – praeito amžiaus paskutinio dešimtmečio viduryje pradėjo nežmoniškai augti. Per dešimt metų, pradedant 1997-aisiais, visame pasaulyje cirkuliuojančių kortelių skaičius išaugo nuo šiek tiek mažiau nei 1,5 milijardo iki 3 milijardų, o vidutinė skola tarp labiausiai įpratusių jomis naudotis amerikiečių padvigubėjo nuo 5 000 iki 10 000 dolerių. Bankai dievino mūsų naująjį prisirišimą prie kreditinių kortelių, kadangi faktiškai, esant nulinei palūkanų normai, jie vis vien patenkinti imdavo nuo 5 iki 30 procentų. Britanijoje „Barclaycard“* kompanijos vadovas specialiam parlamentiniam komitetui prisipažino, kad jis „nesiskolina su kreditinėmis kortelėmis, nes tai per daug brangu“.

Kitos pasaulio šalys nelabai skubėjo pereiti prie kreditinių kortelių. Vakarų Europa tradiciškai vengė plėšikiškos ekonomikos, kuri taip apkerėjo Ameriką ir Britaniją. Todėl ten buvo mažiau kreditinių kortelių turėtojų, taigi mažiau ir asmeninių skolų. Rytų Europoje nebuvo nei pakankamai kapitalo vienam gyventojui, nei saugios

* Pasaulinis kreditinių kortelių ir paskolų teikėjas.

bankininkystės sistemos kreditinėms kortelėms valdyti. Kreditinės kortelės pokomunistiniame pasaulyje buvo retenybė, žaisliukas, tinkamas naujųjų rusų – saujelės gyventojų, kurie susikrovė kvapą gniaužiančias pinigų sumas, plėšdami savo šalis ir tėvynainius pereinamuoju nuo komunizmo į kapitalizmą laikotarpiu, – užmačioms vykdyti.

Tačiau anglosaksiškoje kazino tipo dvidešimto amžiaus paskutinio dešimtmečio ir dvidešimt pirmo amžiaus pirmo dešimtmečio ekonomikoje kreditinių kortelių išradimas prilygo pinigų spausdinimo išradimui. Jo autorės – finansinės institucijos – ilgai nelaukusios ėmė kasinėti šiuos turtingus klodus. Tonos informacinių lapelių kas dieną buvo išsiunčiamos Vakarų pasaulio adresatams, raginant žmones pasirašyti sutartis įsigyti kreditines korteles arba perkelti turimą skolą į naują sąskaitą, kuriai šešis mėnesius nebus priskaičiuojamos palūkanos. Uolesni klientai sugebėdavo išvengti palūkanų už kreditus iki trejų ar ketverių metų, perkeldami savo įsiskolinimo likutį iš vienos kortelės į kitą. Tuo pat metu bankai dėjo kas kartą didesnes pastangas, norėdami pritraukti naujų klientų.

Daugybė kortelių. Daugybė pinigų, su kuriais galima žaisti. Kadangi internete „klajojo" tokie didžiuliai elektroniniai turtai, ko gero, neverta stebėtis, kad jie pradėjo traukti kompiuterininkų iš Rytų dėmesį. Pastarieji neturėjo pinigų, bet jų techninis sumanumas liejosi per kraštus. Vienas iš jų buvo Skriptas, aštuoniolikmetis Dimitrijus Golubovas iš Odesos.

Taip gimė kibernetinių sukčių planeta „CarderPlanet".

5
Karderių planeta

Blyksinčiame „Žvaigždžių karų“ scenarijaus teksto fone pamažu išryškėja klausimas:

IEŠKOTE PROFESIONALAUS SPRENDIMO?

Kadre priartėja greitai besisukanti Žemė ir, lydint veržliai elektroninei šokių muzikai, sprogsta ir virsta metaline psichodeline mozaika.

Tada pasirodo eilė žinučių:

ATRASK TECHNOLOGIJŲ GALIĄ
JAUTIESI PAVARGĘS NUO KASDIENĖS RUTINOS?
NORI PAKEISTI SAVO GYVENIMO BŪDĄ?
TAPK VIENU IŠ MŪSŲ!
TAU NESISEKA?
KREDITINĖS KORTELĖS GALI PADARYTI TAVE TURTINGĄ!

Ekranas gęsta ir tamsėja, o tada pasirodo dar trys pranešimai, kuriuos paryškina bosiniai karo būgno garsai:

KOMANDA, KURIA GALI PASIKLIAUTI
Bum!
VISKAS, KO REIKIA VERSLUI
Bum!
„CarderPlanet“ NEIŠVENGIAMA
Bum!

2001-aisiais buvo įkurta sukčiautojų kreditinėmis kortelėmis planeta „CarderPlanet“, o praėjus metams Skriptas sukvietė savo draugus programišius į Pirmąją pasaulinę karderių konferenciją Odesoje – į pirmąjį kada nors įvykusį kibernetinių nusikaltėlių suvažiavimą – atšvęsti novatoriškos internetinės svetainės gimimo. Ši grupė galėjo pasigirti tokiais pat neįtikėtinais kompiuteriniais sugebėjimais kaip ir „Programišių respublika“ – slapta grupė, kuriai priklausė svarbiausia populiaraus Stiego Larssono romano *Mergina su drakono tatuiruote* (*The Girl with the Dragon Tattoo*) veikėja Lisbetha Salander, pravarde Vapsva.

Bet Skriptas ir jo draugai nebuvo pramanyti. Karderių planeta iš tiesų egzistavo.

6
Šeimos afera

Pirmojoje pasaulinėje karderių konferencijoje buvo atšvęstas pirmasis „CarderPlanet“ gimtadienis. Jis buvo unikalus ir nepaprastas. 2002-aisiais Odesa jau buvo aprimusi – netgi atsirado normalaus miesto požymių. Jos išgarbintoje gatvėje Deribasovskaja knibždėte knibždėjo gatvės pardavėjų, kaip grybų po lietaus pridygo parduotuvių ir prabangių restoranų. Viename iš pirmųjų pokomunistinių airiško tipo barų „Mick O'Neill's“ su keturlapiais dobilais apsuptu pavadinimu, užrašytu gėlų kalba, įtakingas Ukrainos aukščiausio rango programišių branduolys, pasivadinęs Šeima, aptarinėjo konferencijos tikslus. Ten buvo tokios pagrindinės figūros kaip Auditorius, Raidenas ir Stambus Pirkėjas, taip pat šio renginio iniciatoriai: komunikacijų ir saugumo specialistas Smauglys (*Boa*) su įspūdinga balta barzda ir energingas, nors ir šiek tiek paauglišKai atrodantis Skriptas.

Kitas tris dienas jie gėrė ir dainavo keliose skirtingose miesto vietose, bet visų pirma aptarinėjo trumpalaikius ir ilgalaikius savo ką tik užgimusios interneto svetainės „CarderPlanet“, dėl kurios jau keitėsi kompiuterinių nusikaltimų prigimtis visame pasaulyje, vystymo reikalus.

Pagrindinės diskusijos vyko tuo metu pačiame brangiausiame miesto viešbutyje „Odesa“. Aukštas pastatas yra tipiškas neskoningo pokomunistinio prašmatnumo pavyzdys, bet jis bent jau stovi ant molo visai prieš pat Potiomkino laiptus, kurie išgarsėjo

po Eizenšteino ankstyvųjų sovietinių filmų šedevro „Šarvuotis Potiomkinas“. Tarp temų, kurias aptariant „Odesos“ viešbutyje dalyvavo visi delegatai, buvo poreikis išsiaiškinti mažesnės svarbos kreditinių kortelių, tokių kaip „JCB“ ir „Diners“, techninius duomenis. Buvo pastebėta, kad joms nebuvo skirta tiek dėmesio kiek pelningesnėms privilegijuotoms „Visa“ ir „MasterCard“. Taip pat buvo nutarta plėtoti ir stiprinti naujus tinklus žmonių, kurie galėtų išgryninti vogtų kreditinių kortelių pinigus tokiuose regionuose kaip Pietų Amerika, Okeanija ir Afrika. Pagaliau kažkas turėjo imtis tikrų kriminalinių operacijų – pinigų paėmimo iš bankomatų. Šiai rizikingiausiai darbų grandžiai daug proto nereikėjo.

Paslaptingesnės diskusijos, kuriose dalyvavo tik apie penkiolika vadovaujančių karderių, vyko mažame nutriušusiame restoranėlyje prie jūros. Šios grupės tikslas buvo įtikinti delegatus įkurti savo regioninius „CarderPlanet“ franšizės tinklus, kad organizacijos savininkams ir toliau plauktų pinigai, bet jiems reikėtų mažiau dirbti.

Susirinkimui prasidėjus, vienas iš mažiau žinomų delegatų pasiuntė Smaugliui vos pastebimą signalą. Vyriškis atliko elektroninį restorano patikrinimą ir aptiko, kad kambaryje veikia slaptos vaizdo kameros ir skaitmeniniai įrašymo prietaisai. Egzistavo didelė tikimybė, kad juos seka Ukrainos slaptoji policija SBU. O jei renginį stebi SBU, vadinasi, stebi ir Rusijos KGB, kuris tuo metu žvalgyboje jautėsi SBU valdovu – galėjo naršyti po duomenis pirmiau, nei juos patikrins tie, kurie juos surinko.

Šeima, tarsi koks „CarderPlanet“ politinis biuras arba kupolas, ne itin bijojo amerikiečių ir europiečių žvalgybos ir policijos operacijų. Bet KGB buvo visai kas kita, taigi neatsitiktinai pačios svarbiausios konferencijos rezoliucijos pasisakė prieš kenkėjiškus veiksmus Rusijos ir Ukrainos teritorijose. „Mes dar sykį pabrėžiame, kad bet kokie veiksmai prieš mūsų atsiskaitymo sistemas, bankus

ar finansines institucijas yra visiškai neleistini", – griaudėjo Šeima. Jei kas nors iš rusiškai kalbančių kompiuterinių nusikaltėlių imtųsi veiksmų prieš Rusijos bankus ar finansines įmones, visas projektas per penkias minutes būtų nutrauktas.

Tačiau „CarderPlanet" pasirodė ilgaamžiškesnė. Interneto svetainė egzistavo beveik ketverius metus. Neperdėsime pasakę, kad jos įkūrėjai buvo atsakingi už visiškai naujo kriminalinės veiklos metodo atsiradimą ir įtvirtinimą. Tai sukčiavimai, kuriuos buvo galima vykdyti milžinišku mastu su minimaliais ištekliais ir minimalia rizika.

Pagrindinis „CarderPlanet" vaidmuo (kurį vėliau pritaikė daugelis jos pasekėjų) buvo vogtų duomenų – kreditinių kortelių numerių ir PIN kodų, banko sąskaitų ir jų slaptažodžių – prekyvietės organizavimas. Jame radosi ir kitų gėrybių, pavyzdžiui, virusų ir padirbtų dokumentų. Iki tol tokia informacija paprastai būdavo keičiamasi per daug triūso reikalaujančius sandėrius tarp dviejų asmenų per ICQ ir IRC – dvi keitimosi trumposiomis žinutėmis programas, kurias labiausiai mėgo programišiai. Kibernetiniai nusikaltėliai, vadinamieji karderiai, brukalo siuntinėtojai („spameriai"), nelegalių skaitytuvų gamintojai ir virusų kūrėjai buvo visai kitokia nusikaltėlių rūšis, kuri skyrėsi nuo tradicinei mafijos struktūrai priklausančių nusikaltėlių. Savo interviu svarbiame Rusijos kibernetinio pogrindžio metraštyje *Xaker.ru* Skriptas juos pavadino „vienišais vilkais". „Jie nesiburia į grupes ir nekuria savo tinklų; kiekvienas dirba atskirai ir sau."

Rusai buvo ne vieninteliai įsilaužėliai į sistemas, kuriantys kompiuterinių nusikaltimų metodus, tačiau „CarderPlanet" suteikė jiems lig šiol sunkiai perprantamos struktūros prieglobstį. Tokia struktūra padėjo šiems vienišiems vilkams suformuoti savanaudžių veikėjų gaujas, sudarančias sąlygas nusikaltimams (ar paprasčiausioms piktadarybėms) vykdyti, o paskui vėl išgaruoti tuščiuose kibernetiniuose

tyrlaukiuose, puikiai užsimaskavus spragsinčioje ir dūzgiančioje interneto aplinkoje, ir pasipriešinti visoms pastangoms nustatyti, kas tokie jie vis dėlto galėtų būti.

Labai greitai „CarderPlanet" nariai pradėjo ją garbinti. „Turite suprasti, – teigė buvęs patarėjas iš vidinio interneto svetainės rato, – kad Karderių planeta yra ne tik informacijos šaltinis. Joje žmonės tiesiog gyveno – paprastai mes ją vadinome Planeta, tarsi tai būtų mūsų namai."

Kadangi pačios svarbiausios elektroninės piktadarybės buvo vagystės, brukalų siuntinėjimas elektroniniu paštu ir panašūs dalykai, ši veiklą neabejotinai traukė rusakalbius programišius patekti į Planetą ir joje „apsigyventi". Vidutinis naudotojas buvo apdovanotas aistra elektronikai, kompiuteriams ir žaidimams, aistra tinklinėms sistemoms ir potraukiu laužtis į kompiuterių sistemas taip, kaip kiti būna apdovanoti aistra sportui.

Tai nebuvo paprasti nusikaltėliai, laikantys „CarderPlanet" priemone, leidžiančia jiems užsiimti savo amatu. Jie sukūrė vyrišką bendruomenę, kurią daugiausia sudarė unikalių gabumų turintys paaugliai ir ką tik į trečią dešimtį įkopę jaunuoliai, besigrumiantys už būvį tuo chaotišku, įstatymų nepaisančiu istoriniu laikotarpiu. Odesoje visus buvo bandoma įtraukti į kokią nors nusikalstamą veiklą, tarsi tai būtų savaime suprantamas dalykas. Bet dauguma natūraliai apsiribojo savo gyvenamąja vieta. Planetos „gyventojai" apsiginklavo išgyvenimo logika, susiformavusia per Odesos politinę ir ekonominę sumaištį, ir tuos elgesio modelius pritaikė kibernetinėje erdvėje. Jie nebuvo banditai iš prigimties, jų prigimtį formavo troškimas išgyventi.

Nauja svetainė buvo suskirstyta į atskiras kategorijas, kurių kiekviena buvo skirta tam tikram internetinių nusikaltimų ar įsilaužimų į sistemas aspektui. Kai vienas iš jaunųjų Odesos programišių prisijungė prie „CarderPlanet", jis buvo priblokštas. „Prisiekiu,

jog tai buvo toks pat pojūtis, kokį turėjo patirti Ali Baba, kai pirmą sykį atvėręs olą pamatė ją pilną prigrūstą brangenybių. Kiekviename skyriuje buvo daugybė informacijos, kurią panaudojus buvo galima tapti labai turtingam, net nepakilus nuo savo kompiuterio!"

Pirmaisiais metais šimtai rusakalbių programišių pradėjo tyrinėti svetainę, suvilioti jos įdomios grafikos ir veiksmingo valdymo. „CarderPlanet" logotipe puikavosi cigarą rūkantis ir akį merkiantis džentelmenas – tiksli akiplėšos ir sukčiaus Flašo Hario kopija iš klasikinės pokario komedijos „Šv. Trinijano gražuolės", kurį vaidino George'as Cole'as.

„Tokiems kaip aš, paprastiems berniokams iš provincijos, kurie geriausiu atveju galėjo tikėtis per mėnesį uždirbti šimtą dolerių, – tvirtino jaunas programišius iš Odesos, – finansinis pažadas, išreikštas nežinoma kalba su tokiais žodžiais kaip *Dumps*, *Drops*, *Wires*, *COBs**, buvo hipnotizuojantis."

Svetainė buvo atvira ne visiems. Norint prieiti prie jos „sienomis" aptvertų sričių, reikėjo tapti jos nariu, t. y. pereiti administratoriaus patikrinimą. Pirmaisiais „CarderPlanet" veiklos metais dar keturi vyrukai, be Skripto, ėmėsi šio privilegijuoto vaidmens, tarp jų ir įtakingiausias Skripto kolega Smauglys.

Be kitų užduočių, administratoriaus pareiga buvo nuspręsti, kam turėtų būti suteikta narystė, o kam ne. Visų pirma šios saugumo priemonės buvo sugalvotos tam, kad apsaugotų nuo viso pasaulio įstatymų priežiūros ir žvalgybos institucijų. JAV slaptoji tarnyba ir Britanijos slaptoji žvalgybos tarnyba buvo gerai susipažinusios su „CarderPlanet" pirmtakais „carder.org" ir „carder.ru". Skriptas buvo pasiryžęs šį sykį jų arti neprisileisti. Jis buvo tikras, kad vietinė Ukrainos policija nesukels didelės grėsmės interneto svetainei. „Jie niekuo neaprūpinti, nei personalu, nei ištekliais, – teigė jis. – Niekas

* Programišių tarpusavio slengas – žodžiai turi kitą prasmę nei tiesioginė.

Ukrainos įstaigose gerai nemoka anglų kalbos ir vargu ar jie išvis ką nors apie tai nutuokia. Todėl net ir gavę informacijos iš „priešų", tai yra iš mūsų, jie jos nesupras (ir negaus pinigų tam reikalui), taigi iš esmės jie apskritai neturės ką svarstyti."

Uolesni už Ukrainos policininkus buvo jų kolegos iš Rusijos, iš Vidaus reikalų ministerijos R departamento, kuris vėliau buvo reorganizuotas ir galiausiai vėl atsirado kaip K departamentas, užsiimantis visais su moderniomis technologijomis susijusiais nusikaltimais. Rusijos slaptoji policija prasiskverbė į „CarderPlanet" ir sukėlė jai pavojų beveik tuojau pat, kai ši buvo įkurta. Bet, kaip pareiškė internetinis sukčius iš Baltarusijos, vadinamas Policijos Šunimi: „Jei mes patys nepadarysime netvarkos prie savo durų, mūsų vietinė policija ir žvalgybos tarnybos neturės dėl mūsų problemų." Kodėl KGB turėtų švaistyti savo išteklius ir tyrinėti interneto tinklus, kurie grobia pinigus iš amerikiečių ir europiečių kreditinių kortelių? Absoliutus laiko švaistymas. Taigi tuo metu Maskva tenkinosi stebėdama ir išsaugodama informaciją. Ji tiksliai žinojo, kas yra kas Odesos kompiuterinių sukčių bendruomenėje.

Ironiška tai, kad nors „CarderPlanet" ir kibernetiniai nusikaltėliai didžiavosi, jog socialiniu, kultūriniu ir psichologiniu požiūriu jie labai skiriasi nuo tradicinių nusikaltėlių sindikatų, Skriptas ir jo bendrai, formuodami savo organizacijos struktūrą, vis tiek nusprendė pasitelkti Sicilijos mafijos terminologiją. Vėliau karderiai apmąstė, kad panaudoti tokią akivaizdžią kriminalinę metaforą nebuvo išmintingas sprendimas, nors tomis ankstyvomis jų gyvavimo dienomis tiksliame Skripto psichologiniame aprašyme ir jo ateities troškimų išsakymuose buvo galima rasti užuominų apie jo siekį vadovauti galingam socialiniam judėjimui.

Svarbiausias pareigas užimantys nariai (visada ne daugiau nei šeši) priklausė Šeimai, kurios aukščiausiam atstovui, arba administratoriui, buvo suteikiamas Krikštatėvio vardas. Jei tik šis Šeimos

vadas kam nors duodavo leidimą patekti į Planetą, toks narys galėdavo tyrinėti įvairias svetainės sritis. Pavyzdžiui, vienoje jos dalyje jis galėjo peržiūrėti daugybę parduodamų virusų, kuriuos vėliau galėjo panaudoti konkrečiai atakai prieš kitus kompiuterių naudotojus. Virusų kūrėjai taip pat siūlė už pinigus pagal užsakymą sukurti individualias kenkėjiškas programas, kurios galėtų prasiskverbti į tam tikras sistemas ar programas.

Daugiausia veiklos vyko Karderių forume. Šiame skyriuje buvo galima nusipirkti ir parduoti vogtus kreditinių kortelių ir banko sąskaitų rekvizitus. „Dirbdamas šį darbą, – aiškino Skriptas, – karderis gali specializuotis kokioje nors kitoje kardingo srityje. Bet nėra nė vieno, kuris galėtų daryti viską. Anksčiau ar vėliau ir tokiam karderiui prireiks kieno nors kito paslaugų. Štai kodėl reikalingi tinklai ir grupės – žmonės keičiasi informacija ir skaičiais. Tai gali būti bankinės sąskaitos, išsami informacija apie kortelių savininkus, kartais net paso duomenys. Dalį laiko karderiai gali padirbėti kaip įsilaužėliai, nes kartais nepasiseka rasti reikalingos informacijos (nemokant už ją) tol, kol neįsilauži į serverį."

Kitame skyriuje buvo galima nusipirkti vakarietišką pasą arba, tarkim, amerikietiškas vairuotojo teises. Daugeliu atvejų padirbti dokumentai buvo aukščiausios kokybės. Tačiau, būdamas pirkėjas, kaip galite neabejoti šių klastočių kokybe? Ir dar daugiau – kaip galite būti tikras, kad pardavėjas nesiruošia jūsų apiplėšti? Galų gale juk jums ne paslaptis, kad asmuo, iš kurio perkate, yra nusikaltėlis! Jau buvo žinoma, kad internete veikia „plėšikai" – nusikaltėliai, apiplėšiantys kitus nusikaltėlius.

Stipriausias „CarderPlanet" koziris buvo tas, kad Šeimos nariai kontroliavo visą ateinančią ir išeinančią informaciją. Įvedę patikrinimo sistemą, jie dar labiau sustiprino svetainės saugumą, kai padarė ją mokamą, kad neįsileistų visokių atsitiktinių piktadarių. Iš pradžių buvo „didelis antplūdis mėgėjų, kurie tiesiog sukėlė netvarką

forume“ ir kuriais Skriptas norėjo atsikratyti, bet dar daugiau žalos padarė plėšikai, „kurie siūlė žemos kokybės paslaugas arba tiesiog neatliko tų paslaugų, už kurias ėmė pinigus.“

Visgi Planeta nebuvo tik kompiuteriniams vagims skirta universalinė parduotuvė, nes patikrinimo sistema leido administratoriams laiduoti už verslo sandėrius, atliekamus per jų svetainę. Mainais jie sulaukė liaupsių, pinigų ir daug didesnės bei efektyvesnės rinkos savo pačių produktams – visko vienu sykiu.

Nors buvo tikras programišius, nuo kitų Skriptas skyrėsi ir tuo, kad labiausiai jį valdė troškimas užsidirbti pinigų. Kad ir jaunas, jis labai vertino tas marias grynųjų, kuriose maudėsi Vakarų pasaulis, o ypač Amerika. Pelnas yra neabejotinai galinga jėga, tačiau pagrindinis Planetos kūrybinis genijus buvo ne Skriptas, o jo vyresnysis kolega Smauglys, kuriam pinigai buvo antraeilės reikšmės dalykas.

Smauglys kaip asmenybė labai skyrėsi nuo kitų Planetos „gyventojų“. Tuo metu, kai Skriptas sukūrė Planetą, Smauglys buvo beveik keturiasdešimtmetis, taigi gerais dviem dešimtmečiais vyresnis už daugumą savo kolegų, ir daug geriau suprato pasaulį.

Praeito amžiaus devintajame dešimtmetyje, dar tebeegzistuojant Sovietų Sąjungai, Smauglys baigė du universitetus ir taip įrodė esąs talentingas elektronikos studentas. Jis ypač domėjosi mėgėjišku trumpųjų bangų radiju. Tais laikais tai buvo delikatus pomėgis, nes sovietinė žvalgyba (o trumpųjų bangų radijo atveju tai buvo *karinė* žvalgyba) atkakliai siekė kontroliuoti visas į šalį įeinančias ir iš jos išeinančias komunikacijas.

Smauglys buvo labai populiarus, laisvų manierų, kurios akimirksniu galėjo sukurti charizmą. Nors kai kurie draugai manė, kad jis bendradarbiauja su karinės žvalgybos dešifravimo skyriumi, jis vis tiek tapo pasaulinės mėgėjiško radijo brolijos „reklaminiu veidu“. Nesunku įsivaizduoti, kad diduma šiai bendrijai priklausančių vaikinų buvo gana drovūs, bet gabūs keistuoliai.

Smauglys pelnė pasaulinį autoritetą, tapęs pirmuoju mėgėjiško radijo operatoriumi, įvykdžiusiu transliaciją iš uždraustos karo zonos Vietnamo Spratlio salose, o vėliau nustebino dar didesniu laimėjimu – pasiuntė pačius pirmuosius mėgėjiško radijo signalus iš Šiaurės Korėjos. Dėl šio mėgėjiško radijo garsas apie jį pasklido pirmiausia Amerikoje, Europoje ir Australijoje. Jis sutraukdavo didžiules minias gerbėjų, kai praeito amžiaus paskutiniame dešimtmetyje pasirodydavo mėgėjiško radijo aistruolių susirinkimuose. Žmonėms jis instinktyviai patiko, nes buvo išvaizdus ir mokėjo reikšti mintis. Kiekvienas norėjo tapti jo draugu.

1999 m. rudenį, naršydamas internetą, Smauglys atsitiktinai užtiko svetainę „CarderPlanet", ir jam iš karto padarė įspūdį jos verslininkiška, nors ir kiek chaotiška prigimtis. Jis gyveno Maltoje ir jau turėjo sėkmingą pasaulinį verslą: pardavinėjo aukšto lygio sekimo, kovos su sekimu ir kovos su terorizmu technologijas politikams ir verslininkams iš daugiau nei šešiasdešimties viso pasaulio šalių.

Būdamas tikras dėl Smauglio profesinės patirties ir organizacinių gebėjimų, po kelių mėnesių Skriptas pakvietė jį tapti Šeimos nariu. Įkvėptas Skripto veržlumo ir energijos nuo tada, kai pirmą sykį įsidėmėjo svetainę, 2002 m. pradžioje Smauglys sutiko tapti „CarderPlanet" nariu. „Atvykęs į Planetą, Smauglys ją iš esmės atgaivino, – prisiminė vienas iš Planetoje „apsigyvenusių" jaunuolių. – Jis buvo atsakingas už dizaino kokybę ir pristatė keletą naujų skyrių. Jis tapo „vietine" įžymybe."

Tuo pat metu Smauglys sutarė su Skriptu, kad sukurs naują interneto svetainę pavadinimu „Boa factory" (Smauglio fabrikas), kurios veikla papildys svetainės „CarderPlanet" darbą, pagrindinį dėmesį skirdama kitiems prekybos sektoriams – be kitų dalykų, Smauglio fabrikas buvo žinomas dėl savo specializacijos padirbinėjant pasus ir asmens tapatybės korteles, taip pat dėl labiau išvystytos klonuotų kreditinių kortelių ir nuo jų nuskaitytų duomenų mažmeninės prekybos.

„Boa factory" buvo grynai verslo svetainė, o „CarderPlanet" akcentavo socialinį pogrindžio aspektą: atskiri karderiai galėjo susitikti internete, pasikalbėti, pirkti ir parduoti.

Smauglio fabrikas sukūrė priemonę, kuri sukėlė perversmą; ją vėliau perėmė ir Karderių planeta, o kibernetiniai nusikaltimai ėmė augti pramoniniu mastu. Didžiausias iššūkis, su kuriuo susiduria kompiuteriniai vagys, yra susijęs su žinojimu, jog asmuo, su kuriuo jie turi verslo reikalų, irgi yra kriminalinis nusikaltėlis ir jau vien dėl to yra nepatikimas. Kad būtų galima išspręsti šią problemą, Smauglys sugalvojo sąlyginių įsipareigojimų sistemą, kuri iš pradžių vadinosi Garantine tarnyba. Pardavėjas pateikia šios tarnybos „pareigūnui" savo prekių pavyzdžius (tarkim, tuziną kreditinių kortelių numerių ir PIN kodų), o potencialus pirkėjas tuo pat metu atsiunčia jam pinigus. Tada „pareigūnas" patikrina prekes ir, jei žadėtieji pinigai atėję, perveda juos pardavėjui, o kreditinių kortelių duomenis – pirkėjui. Pasitvirtino, kad šis paprastas mechanizmas – genialus. Nuo tada prekyba pasidarė saugi ir todėl smarkiai išaugo.

Mintis sukviesti visą Šeimą į Pirmąją pasaulinę karderių konferenciją 2002 m. vasarą taip pat gimė Smaugliui. Taigi kai kvietimas apsilankyti Odesoje buvo pamėtėtas ant elektroninių „durų kilimėlių" visoje buvusioje Sovietų Sąjungoje, jo gavėjai trokšte troško susimokėti už lėktuvo bilietą į pietus (nors natūralu tikėtis, kad jie beveik neabejotinai už jį mokėjo iš kieno nors kito kortelės). Argi katalikas praleistų progą aplankyti Lurdą? Arba musulmonas galimybę pamatyti Meką? Aišku, kad ir joks save gerbiantis nusikaltėlis neatsisakytų pasiūlymo savaitę praleisti Odesoje.

Planeta pasiekė savo sėkmės viršūnę. Jos „gyventojai" gyrėsi galimybėmis „pasidaryti" pinigų, o šimtai programišių, įsilaužėlių ir brukalo siuntinėtojų nervingai laukė, ar Kupolas suteiks jiems vertingą narystės privilegiją.

Skriptas pradėjo susirinkimą, duodamas pirmą viešą interviu svarbiausiam kibernetinių sukčių žurnalui *Xaker.ru*, kuris yra leidžiamas iki šiol ir tebėra Rusijos pogrindininkų biblija, bet netgi jo skaitytojai buvo šokiruoti, matydami, kaip 2002 m. kovą Skriptas atskleidžia Planetos paslaptis. „Kas skatina kokį nors žmogų tapti karderiu?“ – paklausė Skripto žurnalistas, atkreipęs dėmesį į tai, kad visiems žinomas Rusijos departamentas R buvo sukurtas būtent kovoti su jais ir į juos panašiais nusikaltėliais.

Skriptas: Jie klauso savo širdies ir proto balso. Mokslas įrodė, kad žmonės, kurie nebijo rizikuoti, patiria vadinamojo laimės hormono antplūdį. Tas hormonas, kurio veikimą sustiprina tam tikras kiekis šlamančių dolerių, vaidina pagrindinį, lemiamą vaidmenį, skatinantį tam tikrą žmogų tęsti darbą šioje ne visai sąžiningoje srityje.

Žurnalas: Nejaučiant kaltės?

Skriptas: Nejaučiant kaltės. Ne tik todėl, kad bet kokį mokėjimą bet kas gali atšaukti netgi praėjus daug laiko, paprasčiausiai nusiųsdamas bankui atitinkamą pareiškimą, bet taip pat ir todėl, kad kardingas nėra toks baisus užsiėmimas, kaip kai kam gali atrodyti. Jis kur kas mažiau gėdingas nei plėšikavimas. Kortelių turėtojams mes nesukeliame jokių problemų – viską iki paskutinio penso jie gali atgauti iš bankų, jei tik to paprašys. Tai mūsų vyriausybė turėtų jaustis kalta dėl to, kad paaugliai išmoksta švaistyti pinigus būdami tokio jauno amžiaus.

Golubovas stengėsi racionaliai paaiškinti šį verslą, kaip tai daro dauguma sukčiautojų kreditinėmis kortelėmis: bankai visada sumokės pinigus, taigi paprasti žmonės nenukentės. Toks sentimentalus, populistinis tuščiažodžiavimas parankus tiems, kurie nenori pastebėti, kad dėl sukčiavimo patirtus nuostolius bankai perkelia ant savo klientų pečių, taigi tie sukčiai tiesiogiai kenkia paprastiems žmonėms, kuriais Skriptas tariamai taip rūpinasi.

Šiaip ar taip, jo mintis apie tai, kad vyriausybėms nė kiek nerūpi, kad tiek daug paauglių nueina nusikalstamais keliais, verta apmąstymo. Ukrainoje mafija buvo gana tvirtai įsišaknijusi ir šalies vadovaujantieji politikai ir verslininkai rodė pasibaisėtiną pavyzdį, kuriuo Skriptas iš tiesų uoliai sekė.

Nusistatęs prieš esamą aplinką, Skriptas tikėjo, jog Karderių planetoje sugebės apsirūpinti pakankama pinigų suma, kad galėtų patekti į aukštesnę Ukrainos verslo lygą. Jį valdė ne kas kita, kaip tik ambicijos. O kodėl gi jam galėtų nepavykti?

7
Smauglys prismaugtas

Maždaug tuo laiku, kai Skriptas Odesoje paleido į gyvenimą „CarderPlanet“, programinės įrangos gigantas „Autodesk“, kurio būstinė yra San Rafaelyje, Kalifornijoje, nusprendė, kad jau pats laikas kreiptis į FTB. Didžiausia pasaulinė programinės įrangos, skirtos projektuoti 2D ir 3D formatais, gamintoja „Autodesk“ parduoda savo gaminius viso pasaulio architektams, projektuotojams, miestų planavimo specialistams, modeliuotojams, hipotekos brokeriams, transporto priemonių gamintojams – ką gi, net ir Skantorpo cheminės inžinerijos firma „Grimley Smith Associates“ pasirinko juos programinės įrangos tiekėjais.

Tokia speciali programinė įranga nėra pigi. Viena „Autodesk“ gamybos profesionalaus projektavimo programų paketo CAD licencija kainuoja nuo 3 000 iki 7 000 dolerių. Taip yra todėl, kad į produkto mokslinius tyrimus ir tobulinimą investuojamos didžiulės sumos.

2002 m. kompanijos Apsaugos nuo piratavimo skyriuje buvo pastebėta, kad pardavėjas iš Ukrainos siūlo naujutėles vienos „Autodesk“ projektavimo programos versijas per „eBay“ už nedidelę 200 dolerių kainą, nors ta pati prekė mažmeninės prekybos parduotuvėse kainuoja 3 500 dolerių. „Hmm, – pamanė jie, – čia kažkas negerai!“

Silicio slėnis susiduria su tokiomis pat problemomis kaip ir Holivudo studijos. Filmui pastatyti reikalingas lėšas dažnai galima palyginti su tomis, kurios reikalingos sudėtingai programinei įrangai

sukurti. Augant gamybos sąnaudoms, pasaulinio padirbtų skaitmeninių universaliųjų diskų (DVD) gamintojų tinklo, dažnai turinčio ryšių su organizuotų nusikaltėlių sindikatais, atsiradimas sumažino pajamas iš kino filmų. Tai ypač pasakytina apie ekonominės recesijos periodą – jei turite galimybę rinktis, ar išleisti 15 dolerių, kad pažiūrėtumėte filmą kino teatre, ar pasižiūrėti jį puikiai nukopijuotą į DVD už 1 dolerį ir netgi dviem mėnesiais anksčiau, nei jis rodomas kino teatruose, pastarajai galimybei sunku atsispirti.

Arba, tarkim, jūs valdote konkurencingos srities įmonę ir jums reikia turėti „Autodesk" produktų. Kad įsigytumėte būtiną programinę įrangą ir licencijas iš kompanijos, jums gali tekti pakloti beveik 20 000 dolerių, bet jei pirktumėte jas iš šio ukrainiečio per „eBay", iš viso išleistumėte tik 800 dolerių. Būkime atviri: gal tai ir nelegalu, bet vilioja!

Nuo praeito amžiaus aštuntojo dešimtmečio, kai tik buvo pradėta prekiauti programine įranga, jos gamintojai bergždžiai stengiasi sukurti technologiją, kuri galėtų apsaugoti ją nuo galimybės nukopijuoti. Tą patį jie bandė padaryti ir su kompaktiniais diskais (CD) bei skaitmeniniais universaliaisiais diskais. Nė viena šios rūšies technologija neatsilaikė ilgiau nei kelias dienas: į ją kaipmat įsilaužda vienas iš dešimčių tūkstančių viso pasaulio programišių ir įsilaužėlių. Per tris pastaruosius dešimtmečius tai pasirodė besanti viena iš labiausiai donkichotiškų moderniųjų technologijų pramonės šakų.

Rytų Europos programišių vaidmuo įsilaužiant į programinės įrangos apsaugos mechanizmus buvo itin svarbus. Devintajame dešimtmetyje, prieš sugriūvant komunistinei sistemai, Sovietų Sąjunga įvairiems savo prekybos bloko – Ekonominės savitarpio pagalbos tarybos – sąjungininkams, ypač Bulgarijai ir Rytų Vokietijai, buvo davusi užduotis išvystyti personalinių kompiuterių ir programinės įrangos pramonę. Komunistiniams kompiuteriams buvo būdingos

tos pačios savybės kaip ir visiems Rytų bloko gaminiams: jie buvo bjaurūs ir nuolatos gedo. Regione naujai atsirandantiems kompiuterių inžinieriams iškelti uždaviniai buvo tokie sudėtingi, kad, siekdami išvengti gedimų ir virusų, jie turėjo parodyti išskirtinį sumanumą.

Dar daugiau – programinės įrangos gamyklos, kurias Rytų europiečiai pastatė devintame dešimtmetyje, po Berlyno sienos griuvimo praeito amžiaus paskutiniame dešimtmetyje negalėjo konkuruoti su Silicio slėniu – investuoti į mokslinius tyrimus ar įrangą nebuvo pinigų. Bet galingi naujai organizuoti nusikaltėlių sindikatai, pademonstravę tokią milžinišką įtaką buvusių komunistinių šalių ekonomikai, šiose gamyklose matė puikias galimybes. Pirmiausia jie įsigijo infrastruktūras (dažniau nesąžiningu, nei doru būdu), o tada įdarbino jose tuos gabius inžinierius, kad jie pramoniniu būdu gamintų programinės įrangos klastotes. Šios gamybos tempus diktavo Bulgarija, Ukraina ir Rusija, o nuo jų nedaug atsiliko ir Rumunija.

Taigi natūralu, kad pastebėjusi, jog vienas pardavėjas iš Ukrainos „eBay" svetainėje siūlo didžiulius kiekius padirbtų jų gaminio versijų pirkėjams Jungtinėse Valstijose, „Autodesk" pajuto pareigą imtis kokių nors priemonių. Kiek pasvarstę jie paskambino į FTB, o FTB savo ruožtu įspėjo San Chosė prokuratūrą Kalifornijoje. Kadangi sukčiavimai buvo susiję su „eBay", iš prokuratūros buvo paskambinta vienam ypatingam tyrėjui – Gregui Crabbui iš JAV pašto inspekcijos tarnybos, kuris tuo metu dirbo San Fransiske.

Yra trys pagrindinės Amerikos teisėsaugos institucijos, įgaliotos spręsti kibernetines bylas: FTB (nes jo darbas yra stabdyti nusikalstamumą), Slaptoji tarnyba (kadangi tarp jos funkcijų yra ir JAV valiutos apsauga bei sukčiavimai su kreditinėmis kortelėmis) ir Pašto inspekcijos tarnyba (nes jos darbas yra kontroliuoti bet kokią nelegalią veiklą, susijusią su Federaline pašto tarnyba). Pastaroji į

kibernetinį žaidimą buvo įtraukta pirmiausia, kadangi sukčiaujant per „eBay“ ir panašias svetaines, prekės dažnai siunčiamos paštu (tiek legaliai perkant, tiek plaunant sukčių pinigus).

Per pastaruosius penkiolika metų JAV pašto inspekcijos tarnyba suformavo atsidavusią komandą, tiriančią su moderniomis technologijomis susijusius nusikaltimus, o Gregui Crabbui taip gerai sekėsi, kad galiausiai iš San Fransisko jį perkėlė į Vašingtoną – vadovauti šios tarnybos Pasaulinių kibernetinių tyrimų skyriui iš didžiulio anoniminio pastato, esančio dideliame anoniminių pastatų komplekse, vadinamame Federaliniu centru (atvykę į JAV sostinę, neužmirškite išbraukti jo iš būtinų aplankyti objektų sąrašo).

Crabbo teutoniška* išvaizda ir girgždoka lėta kalbėsena vienu metu ir traukia, ir baugina. Jis turi diplomuoto buhalterio kvalifikaciją. Į jį pažvelgus sunku atsikratyti įspūdžio, kad jei tik jis peržiūrėtų jūsų finansus, jam nereikėtų ilgai gaišti, kad surastų stambaus įstatymo pažeidimo įrodymų, net jei esate absoliučiai švarus. Ši savybė suteikia Crabbui apčiuopiamą profesinį pranašumą, kadangi gebėjimas išstudijuoti ilgus skaičių bei trumpų pranešimų sąrašus ir iš pirmo žvilgsnio nesuprantamus duomenis geram kibernetinių bylų policininkui yra būtina sąlyga. Darbas gal ir gali atrodyti įdomus, bet, kaip ir dauguma su kompiuteriais susijusių darbų, iš tikrųjų yra sunkus ir nuobodus.

Crabbas įsigilino į „Autodesk“ atvejį ir atsekė sukčiavimą, patikrinęs, kur falsifikuotų programų pirkėjai siunčia savo pinigus. Paaiškėjo, kad jie perveda apmokėjimus į bankų sąskaitas, priklausančias penkiolikai „mulų“ – po visą šalį išsibarsčiusių JAV gyventojų. Pinigų plovimas ir sukčiavimas priklausė nuo tų daugiausia atsitiktinių asmenų, kurie atsiliepdavo į skelbimus, siūlančius gerą atlygį už darbą, atliekamą iš namuose esančio asmeninio kompiuterio. Tada

* Senovės germanų.

laimingiesiems kandidatams būdavo liepiama perduoti savo banko sąskaitas naujųjų darbdavių dispozicijai. „Autodesk" atveju „mulai" gaudavo 200 dolerių, o tada 180 dolerių persiųsdavo, pasilikę sau 20 dolerių komisinių. Pinigus jie siųsdavo į banką Latvijoje, vienoje iš trijų Baltijos valstybių, kurių vaidmuo tiek kibernetiniuose nusikaltimuose, tiek platesnėje kibernetinės apsaugos srityje buvo neproporcingai didelis, palyginti su jų bendru gyventojų skaičiumi (septyni milijonai).

Padedamas Latvijos policijos, Crabbas sužinojo, kad galiausiai pinigai patenka į bankų sąskaitas Ternopilyje, Vakarų Ukrainoje. Visos šios sąskaitos priklausė kažkokiam Maksimui Kovalčiukui arba jo žmonai.

Crabbas išsiaiškino, kad pats Kovalčiukas nesiruošia pakenkti JAV ekonomikai. Pagal pagrindinių organizuotų nusikalstamų grupuočių standartus, „Autodesk" apmaudui, iš savo konkrečių suktybių jis uždirbdavo skatikus. Tada Crabbas nutarė padirbėti ir įsilaužti į Kovalčiuko elektroninį paštą, norėdamas pažiūrėti, ar ten neras kokių nors kitų paslapčių, ir kažkuriuo momentu jam pasitaikė „unikali galimybė" tikrinti Kovalčiuko bendravimą elektroniniu paštu. Vadinasi, Crabbas arba įsilaužė į savo tyrimo objekto kompiuterį, arba įtikino Kovalčiuko elektroninio pašto paslaugos teikėją, kad šis suteiktų jam prieigą. Kad ir kaip ten buvo, ta „unikali galimybė" turėjo toli siekiantį poveikį realiame pasaulyje, kadangi vos pradėjęs skaityti žinutes Crabbas suprato, kad Kovalčiukas įsitraukęs į daug didesnį projektą nei „Autodesk" apgaudinėjimas, o būtent – į internetinės svetainės „CarderPlanet" plėtrą.

Nors pagrindinis šio tyrimo tikslas ir toliau išliko Kovalčiukas ir jo suktybės, Crabbas taip pat pradėjo sudarinėti Karderių planetos Šeimos medį. Nežinodamas, kad jį seka JAV tarnyba, Kovalčiukas bendravo nesivaržydamas, taigi sėkmė ir kruopštus tiriamasis darbas leido Crabbui atsidurti pavydėtinoje padėtyje. Inspektorius

ne tik pažengė į priekį sekdamas patį Kovalčiuką, bet netgi pralenkė Vakarų žvalgybos tarnybas. Iš dalies įsiskverbus į pačią dinamiškiausią kibernetinių nusikaltimų bendruomenę pasaulyje, jam pavyko padaryti tai, ko iki šiol neįstengė Vakarų šnipai.

Nors Crabbas ir sugebėjo daug sužinoti apie tai, kas vyksta Ukrainos programišių bendruomenėje, vis dėlto jis ne kažin ką galėjo padaryti. Jis netgi negalėjo suimti Kovalčiuko. Jungtinės Valstijos ne tik neturėjo ekstradicijos sutarties su Ukraina, bet ir politinės aplinkybės, susiklosčiusios šioje milžiniškoje Rytų Europos šalyje, buvo visiškai tam nepalankios. Leonidas Kučma prezidentavo šalyje, kurioje egzistavo platus korumpuotų ryšių tarp oligarchų ir organizuotų nusikalstamų grupuočių tinklas. Dar daugiau, Jungtinės Valstijos konkuravo su Europa ir Rusija dėl įtakos šioje šalyje, o tuo metu gana stiprus konkurencijos vėjas pūtė iš Maskvos. Taigi kol Kovalčiukas gyveno Ukrainoje, jis buvo saugus.

2002 m. pabaigoje, tuo metu, kai inspektorius Crabbas dar tebebuvo San Fransiske, jį iškvietė į „Visos" saugumo skyrių, kurio centrinis biuras taip pat yra šiame mieste. Jų žmones papiktino neįprasta programišiaus vardu Smauglys sėkmė. Per savo plačiai pagarsėjusią svetainę „Boa Factory" jam pasisekė pavogti arba padėti kitiems pavogti dešimtis tūkstančių kreditinių kortelių duomenų. Crabbas pastatė ausis – Smauglio vardą jis žinojo iš įvairių pokalbių, kuriuos buvo matęs Kovalčiuko pokalbių išklotinėse. Juk Kovalčiukas daug ką pirko iš Smauglio fabriko, išmoko ten prekybos gudrybių ir kartu aptarinėjo Karderių planetos vystymą. Pašto inspektorius greitai atsekė dvi pagrindines Planetos figūras – Smauglį ir Skriptą. Apdairiai pasinaudojęs Interpolu, jis informavo kitas teisėsaugos tarnybas ir paprašė pranešti, jei jos susidurs su ukrainiečiais, įtariamais su moderniomis technologijomis susijusiais nusikaltimais.

2003 m. vasario pabaigoje Romaną Vegą, grįžtantį iš darbinės kelionės į savo namus Maltoje, vienas draugas pakvietė pasisvečiuo-

ti Nikosijoje, Kipre. Visą vakarą juodu su bičiuliu gėrė ir dalijosi prisiminimais apie savo nuotykius Birmoje 1991 m., kai abu priklausė komandai, vedusiai pirmas mėgėjiško radijo transliacijas iš kariškių valdomos valstybės.

Sugrįžęs į savo kambarį „Castelli" viešbutyje, Vega patyrė nemalonią staigmeną – jo laukė vietinis policijos inspektorius Modestas Poyiadjis. Jis nedelsdamas suėmė ukrainietį kaip bendrininką sukčiaujant su kreditinėmis kortelėmis, nors nusikaltimą buvo įvykdęs kitas svečias iš Ukrainos, kuriam Vega buvo leidęs apsistoti savo kambaryje (kaip išaiškėjo, tai buvo netikęs sprendimas). Vegai tai reiškė santykių su teisėsaugos institucijomis Kipre ir Jungtinėse Valstijose pradžią, o tuos santykius galima apibūdinti ne kaip kitaip, kaip tik vertais Kafkos plunksnos.

Kai Poyiadjis patikrino Interpolo įrašus, jis susisiekė su Gregu Crabbu, pagrindiniu JAV pareigūnu, tiriančiu Smauglio atvejį. Vyriškiui iš JAV pašto inspekcijos jis pasakė, kad, jo įsitikinimu, Romanas Vega yra ne kas kitas, kaip Smauglys. Crabbas sunkiai galėjo suvaldyti jaudulį. Pokalbiui dar nepasibaigus, mintyse jis jau užsisakinėjo bilietą pirmam skrydžiui į Nikosiją. Tai buvo ne šiaip sau ketinimas pamėginti perduoti kitai valstybei vieną iš pagrindinių „CarderPlanet" iniciatorių. *Jie turi jo nešiojamąjį kompiuterį!* Jeigu kipriečiai sugebėjo išsiaiškinti, kas buvo jo antrasis aš, iš tiesų net nežinodami, su kuo turi reikalą, tik įsivaizduokite, ką toks tyrėjas kaip Crabbas galėjo ištraukti iš šio kompiuterio standžiojo disko.

„Smauglio suėmimas sukėlė didžiulį šoką", – sakė Karderių planetos narys Xhora, išreikšdamas daugelio savo kompiuterinių tėvynainių iš Planetos tuometinius jausmus. Smauglys buvo tas žmogus, kuris pavertė Karderių planetą malonia, o kartu įdomia ir pelninga vieta. Kadangi jis buvo daug vyresnis ir labiau patyręs už likusius Planetos gyventojus, daugelis manė, kad jis išvengs nemalonumų, susijusių su teisėsauga.

Tuo pat metu Skriptas, turėdamas valdžią Karderių planetoje, didino savo galią ir kaupė turtus. „Jo interviu turėjo tikslą išpopuliarinti svetainę ir išplėsti jo paties verslą, – sakė kitas kompiuterių entuziastas slapyvardžiu Bevardis, – ir jam tai pavyko. Į svetainę plūdo nauji nariai. Bet atmosfera pasikeitė. Ji nebebuvo tokia kaip anksčiau."

Pradžioje buvusi maloni „CarderPlanet" bičiulystė iš tiesų sparčiai nyko. Vis dėlto interneto svetainė generavo daugiau pinigų nei kada nors anksčiau. Buvo įkurta forumo sekcija anglų kalba ir netrukus karderiai iš viso pasaulio jau registravosi į svetainę. O tolimajame San Fransiske Gregas Crabbas „puotavo" prie Smauglio standžiojo disko, atrasdamas jame tūkstančius paslapčių, kuriomis keitėsi Smauglys ir Skriptas. „Man niekada neprisireikė apklausti Smauglio, – sakė Crabbas. – Man net ir neįdomu, ką vaikinas būtų galėjęs pasakyti, nes aš turėjau jo standųjį diską, taigi jis man negalėjo papasakoti nieko naujo!"

Iš tiesų Crabbas gal ir neatrado kompiuteryje visko, ką norėjo rasti. Matyt, kažkuriuo momentu JAV teisėsauga įsilaužė į vieną šifravimo sistemą „Sony" firmos VAIO nešiojamajame kompiuteryje, tačiau savininkas Smauglys buvo jį sustiprinęs galinga sistema „Handy Bits EasyCrypto" (ją galima parsisiųsti nemokamai), kuri turėjo užkirsti kelią prieigai prie maždaug 80 procentų kompiuterio failų.

Karderių forumuose iki šiol išlikęs kartėlis, kadangi nariai mano, jog Romanas Vega išdavė Golubovą. Tai netiesa – visa informacija apie Golubovą buvo išgauta iš VAIO kompiuterio. Vega ne tik tebetyli, nors tai jam kainuoja daug pastangų, bet dabar jis yra jau beveik dešimtmetį praleidęs įvairiuose Kipro ir Amerikos kalėjimuose, nors niekada nebuvo nuteistas už jokį nusikaltimą.

Net ir turėdamas visą naują informaciją Crabbas vis dar nieko negalėjo padaryti Skriptui. Jis buvo Ukrainoje – ne taip kaip Mak-

simas Kovalčiukas, kuris kartu su žmona už sukčiavimą su „Autodesk“ produktais buvo suimtas pieno bare Bankoke, praėjus trims mėnesiams nuo Romano Vegos sulaikymo Nikosijoje. Lygiai kaip Vega iš Kipro buvo perduotas Kalifornijai, taip ir Kovalčiukas iš Tailando buvo perduotas Vakarų pakrantei.

Skriptas neketino išvykti iš gimtosios šalies ir, norėdamas dar labiau apsisaugoti, 2004 m. pradžioje per „CarderPlanet“ paskelbė, kad atsistatydina iš vadovaujamųjų pareigų ir geruoju palieka svetainę.

Skriptas, kaip visada, turėjo planą. Užsiimdamas kardingu, jis jau buvo „pasidaręs“ pakankamai pinigų ir, kaip pamenate, apibūdino juos kaip nekaltai uždirbtus, o dabar norėjo juos investuoti į legalų verslą. Galbūt tikėjosi užbėgti už akių ateityje jo laukiantiems nemalonumams. Gal turėjo ambicijų, nesusijusių su kibernetine sfera. Jis padarė stulbinantį pareiškimą per „CarderPlanet“ – svetainės administravimą jis perduos patikimam patarėjui ir daugiau nevadovaus Planetos tarybai.

Atrodo, kad Skriptas elgėsi garbingai. Tačiau įvyko vienas dalykas, kurio jis nesitikėjo – revoliucija.

8
Scenarijaus perrašymas

Borisas Borisovičius Popovas sukvietė savo tarnybą, kad pranešti, jog nesveikuoja. Jis paaiškino, kad gydytojas jam liepė keletą dienų nepersidirbti. Kai kurie kolegos nustebo. Dėl liekno sudėjimo ir paauglišku bruožų Borisas Borisovičius kartais atrodydavo panašus į liguistą vaiką, tačiau iš tiesų jis buvo bene darbščiausias ir labiausiai disciplinuotas iš visų šių vyrų. „Dirbti su juo buvo grynas malonumas, – vėliau sakė vienas iš jų, – visoje tarnyboje nerastumėte geresnio."

Nors ir atsisakęs dirbti, Popovas neatgulė į lovą, bet sveikas kaip ridikas išėjo iš savo buto, susistabdė taksi ir nuvažiavo į Kijevo Boryspilio oro uostą, kur užsiregistravo skristi į Odesą. Kadangi buvo kilęs iš rytų Ukrainoje esančio Donecko, o jo gimtoji kalba buvo rusų, atvykęs į pietus jis neturėjo sukelti jokių įtarimų, nebent būtų visai praradęs nuovoką.

Atvykęs į Odesą, jis sėdo į autobusą, vežantį į miestą. Buvo karšta liepos mėnesio diena. Temperatūra, ko gero, viršijo trisdešimt laipsnių, tačiau oras buvo malonus dėl lengvo ir švelnaus vėjelio, pučiančio nuo Juodosios jūros. Netrukus Popovas pasiekė privatų butą, kurį buvo išsinuomojęs. Po kelių valandų pasirodė trys jo komandos nariai – Nataša Obrizan ir ponai Griško ir Baranecas. „Mes negalėjome apsistoti viešbutyje, – paaiškino Borisas, – nes nepasitikime vietine policija." Vienintelis žmogus visoje šalyje, kuris žinojo, jog jie yra Odesoje, buvo vidaus reikalų ministras.

Prieš šešis mėnesius Ukraina buvo patyrusi dramatišką sukrėtimą – Oranžinę revoliuciją. Šiai itin derlingai šaliai, turinčiai tokį potencialą, kad daugiau ar mažiau galėtų aprūpinti maistu visą Europos žemyną, dramos nebuvo svetimos. Dėl visų dvidešimto amžiaus režimų, tokių kaip aukščiausio lygio nacionalizmas, autokratija, komunizmas ir fašizmas, šalies gyventojai patyrė baisių negandų: pilietinį karą, masinį badą, genocidą, deportacijas ir plačiai paplitusį skurdą.

Ilgiausiai išsilaikęs šios chaotiškos istorijos vietinis palikimas buvo Ukrainos pasidalijimas į dvi stovyklas – pagal geografinę padėtį ir pagal dvi slavų kalbas – į vakarinę ir rytinę, ukrainietišką ir rusišką dalis. Sostinė Kijevas stovi tarp šių dviejų dalių kaip koks išklibęs tiltas, besitikintis suvesti kartais visai priešiškas tradicijas. Niūriausiomis dvidešimto amžiaus dienomis šalies vakarinė dalis kai kurių žmonių mintyse buvo siejama su fašizmu ir Vokietija, o tuo pat metu rytai buvo laikomi promaskvietiškais ir komunizmo atrama.

Šis suskaidymas ne visuomet labai aiškus – ukrainietiškai kalbančiųjų pinigai kartais atsiduria rytuose, o prorusiški kandidatai dažnai gauna netikėtų balsų iš vakarinės dalies. Vis dėlto tokie neapibrėžtumai yra gana naudingi. Nuo nepriklausomybės paskelbimo Kijevas ir vakarinės Ukrainos sritys dėjo pastangas užmegzti glaudesnius ryšius su Europos Sąjunga ir NATO, o tuo pat metu rytai siekė sustiprinti saitus su Rusija. Ir iš tiesų daugelis rytuose gyvenančių ukrainiečių tebesijaučia visais atžvilgiais priklausomi nuo savo milžinės kaimynės.

Iki 2004 m. besikeičiančios Ukrainos vyriausybės ir vienas po kito renkami prezidentai, dideliam rytinės dalies pasitenkinimui ir vakarų Ukrainos nacionalistų nusivylimui, rėmė prorusišką liniją. Dėl to santykiai su ES, NATO ir JAV buvo šaltoki – Ukrainos valdžios pareigūnai retai pakliūdavo į JAV kalėjimus, apkaltinti pinigų

plovimu ar kita stambia mafijos veikla, ir lygiai taip pat retai lankėsi Baltuosiuose rūmuose.

Tačiau valdžios pareigūnai ir oligarchai prisikimšo kišenes paprastų piliečių sąskaita, o pastarųjų gyvenimo lygis nukrito prieš perėjimą į naują tūkstantmetį ir po jo, todėl naujas politinis judėjimas būrėsi aplink „naujo stiliaus" politikus – Viktorą Juščenką ir Juliją Tymošenko. Tik vėliau paaiškėjo, kad jie buvo panašaus kirpimo kaip ir jų oponentai. Juščenka pateko į laikraščių antraštes 2004 m. rugsėjį, kai kažkas bandė jį nunuodyti dioksinu (buvo beveik neabejojama, kad tai Rusijos kagėbistų darbas). Jis atsilaikė prieš pastangas nunuodyti, nors ir liko žiauriai sudarkytu veidu, ir paskelbė, kad ir toliau sieks laimėti prezidento rinkimus. Kampanija, siekianti išstumti senąją gvardiją, užvaldė jaunųjų ukrainiečių mintis, ir šie pavertė ją politine švente, kurią pavadino Oranžine revoliucija. Studentų aktyvistai iš Balkanuose esančios Serbijos, padėję nuversti savo šalies diktatorių Slobodaną Miloševičių, atvyko į Kijevą, kad pamokytų artimų kaimynų naujuosius gatvės politikus. Naujųjų konservatorių propagandistai iš JAV plūdo į šalį, pajutę galimybę „sukruvinti Maskvai nosį" ir patraukti Ukrainą arčiau NATO orbitos.

Nuo pat pradžių skubių politinių veiksmų banga įgavo tarptautinę reikšmę. Kai 2005 m. sausį Juščenka galiausiai buvo paskelbtas prezidentu, o Tymošenko – ministre pirmininke, Ukraina tapo gyvybiškai svarbiu nuolat blogėjančių Rusijos ir JAV santykių bandomuoju poligonu. Abu naujieji lyderiai ne tik patvirtino Ukrainos pažadą įstoti į Europos Sąjungą, bet taip pat paskelbė turį vilčių, kad šalis netrukus taps NATO nare. Nors tam nebuvo lemta išsipildyti (galiausiai šie siekiai buvo paremti tik 30 procentų ukrainiečių balsų), Maskva jų veiksmus interpretavo ne kitaip, kaip karo paskelbimą.

Per ketverius metus nuo pirmo netikėto susidūrimo su Maksimu Kovalčiuku, žmogumi, kuris pardavinėjo „Autodesk" produktų falsifikatus, inspektorius Gregas Crabbas kantriai plėtojo santykius su

savo kolegomis iš gausybės Ukrainos teisėsaugos tarnybų. Bet kai tik jam pavykdavo užmegzti svarbius ryšius, jie mandagiai atmesdavo jo prašymus sulaikyti Dimitrijų Golubovą, žinomą pravarde Skriptas.

Dramatiški 2004 m. gruodžio ir 2005 m. sausio įvykiai, kai į valdžią atėjo Juščenka ir Tymošenko, visa tai pakeitė. Crabbas suprato, kad Oranžinė revoliucija suteikia jam galimybę, kurios negalima praleisti. Netrukus po audringų įvykių jis sulaukė skambučio iš JAV ambasados Kijeve. Jis sužinojo, kad Ukrainos vidaus reikalų ministerija jau apsivaliusi nuo senųjų kietosios linijos šalininkų ir tarnybą pradėjo nauja komanda, labiau nusiteikusi dirbti su Vakarais. „Greitai atvykite čia!" – buvo jam pasakyta iš ambasados. Vyriškiui iš Pašto inspekcijos tarnybos nereikėjo antro kvietimo.

Jis atvyko į Kijevą 2005 m. birželį ir Vidaus reikalų ministerijos pareigūnams davė parodymus Golubovo byloje. Po dviejų savaičių inspektorius Popovas ir Kovos su organizuotu nusikalstamumu departamento darbuotojai jau buvo kelyje į Odesą, turėdami nurodymus susekti ir suimti nesugaunamąjį Skriptą.

Popovas suprato, kad tai sunki užduotis. Labiau už viską jis bijojo kokio nors informacijos nutekėjimo, nes jei žinia apie reidą pasiektų Odesą anksčiau nei jis pats, visa operacija žlugtų dar nė neprasidėjusi. Kaip patyręs karderis, jau susikrovęs ne vieną milijoną dolerių, Golubovas, reikia manyti, jau buvo nusipirkęs vietinių teisėsaugos tarnybų apsaugą. Tarp savųjų jis buvo neįveikiamas.

Dovženkos gatvė yra maždaug už trijų kilometrų nuo Odesos centro. Gatvės čia apsodintos medžių eilėmis ir ši vieta laikoma viena iš madingesnių mieste. Golubovas gyveno savo močiutės bute, taigi kai Popovas ir jo brigada netikėtai ten atvyko, jie labai nustebo pamatę storo plieno duris, užtvėrusias įėjimą. Užėmus reikiamą poziciją, Popovas davė signalą savo kolegoms. „Atidarykite! Policija!" – šaukė jie, belsdami į nepajudinamas duris. Tvyrant tylai jie įsitempę mėgino ką nors išgirsti už plieninio barjero – vienam iš jų pasirodė,

kad girdi kažkokį šlepsėjimą, bet, nepaisant visų pastangų, durys tebebuvo tvirtai užsklęstos.

Kol Popovas svarstė, ar neišsikvietus kokios nors sunkiosios technikos, jų šnerves pasiekė aitrus degančio popieriaus kvapas. „Viešpatie, – pagalvojo jis, – jis pradėjo naikinti įkalčius!“ Popovas negaišdamas laiko pranešė avarinei tarnybai ir netrukus atvažiavo gaisrinis automobilis. Karščiui didėjant ugniagesys pramušė skylę buto sienoje ir pradėjo pro ją purkšti putas. Kai jau atrodė, kad močiutės butas tuoj tuoj patvins nuo pramoninių chemikalų, Golubovas galiausiai nusprendė, kad žaidimas baigtas, ir atidarė duris.

Reginys buvo nepaprastas. Popovas ne tik pamatė degančius Golubovo užrašus, bet ir patį programišių, „Raskat“ prietaisu naikinantį informaciją iš kompiuterinių diskų. Jei Golubovas būtų paprasčiausiai ištrynęs failus iš įvairių savo kompiuterių, bet kuriam, turinčiam elementarių įgūdžių, kaip iš kompiuterių išgauti kaltės įrodymus, ir norinčiam tuos failus atkurti, tai padaryti nebūtų buvę labai sunku. Lengva sudeginti dokumentus – daug sunkiau sunaikinti kompiuterinius failus. Bet rusų sukonstruotas prietaisas „Raskat“ generuoja galingas elektromagnetines bangas ir gali visiškai sunaikinti duomenis. Golubovas buvo sugautas nusikaltimo vietoje, ir Popovas palydėjo jį į Kijevą, kur jis buvo įkalintas.

Dabar abu – ir Vega, ir Golubovas – buvo uždaryti į kalėjimą (kaip ir keletas kitų svarbių „CarderPlanet“ Šeimos narių). Abu iš paskutiniųjų neigė esą Smauglys ir Skriptas. Nė vienas iš jų dar nepripažintas kaltu – tiesą sakant, pirmasis jau praleido beveik dešimt metų Amerikos kalėjimuose, niekada net nedalyvavęs teismo procese, o tai sukelia rimtų abejonių dėl JAV baudžiamosios teisinės sistemos efektyvumo.

Šiaip ar taip, „CarderPlanet“ buvo įveikta. Mistiška programišių ir įsilaužėlių svetainė gal ir išnyko, bet jos palikimas buvo didžiulis – ji iš pagrindų pakeitė internetinį nusikalstamumą.

Dar daugiau – stambaus masto kibernetiniai nusikaltimai jau buvo peržengę savo ukrainietiškos kilmės ribas. Per paskutinius dvejus „CarderPlanet“ gyvavimo metus administratoriai plėtojo anglakalbių forumą, kuris veikė greta rusiškų diskusijų padalinių. Šis forumas viso pasaulio programišius ir karderius užkrėtė Odesos dvasia. Du jo nariai buvo naujokai, bet juos sudomino šis naujas profesinio kardingo pasaulis. Vienas iš jų pasirinko linksmo pirato įvaizdį, o kitas įsikūnijo į daugelio šiuolaikinių technologijų entuziastų mėgstamo filmo veikėją ir pasivadino slapyvardžiais JiLsi ir Matrix001*.

* *Matrix* – Matrica. (Angl.)

III dalis

9
Tigras, tigras

Kolombas, Šri Lanka, 1988 metai

Bum! Bum! Bum!
– Atidarykit! Atidarykit!

Taip nusiteikę kareiviai retai laukia atsakymo, ypač pusę šešių ryto. Jie išlaužė duris savo šautuvais ir sugriuvo į namą. Tyrinėdami kambarį po kambario, įsakė šeimos nariams sugulti ant grindų, o tada apieškojo gyvenamąją patalpą.

Trys berniukai atsibudo apimti siaubo, kai namus užpildė triukšmas ir šviesa.

– Marš iš lovos! Iš lovos!

Prakaituodami nuo tropinio karščio, vienais apatiniais, vaikai kaleno dantimis iš baimės. Kareiviai ištraukė vyriausią, dar tik vienuolikos metų berniuką ir, rodydami į plaštakos dydžio baltos odos lopą jam ant pilvo, beveik pergalingai šaukė:

– O kas čia? Kas čia? Jis naudojo sprogmenis!

– Tai įgimta žymė, – atsakė jis, – tik įgimta žymė.

Jie patraukė berniuką į šalį ir, pasodinę ant kėdės svetainėje, pradėjo tardyti. Tėvai ir močiutė bandė užtarti jį prieš kareivį, kuris, kaip atrodė, vadovavo operacijai, ir galiausiai šis sutiko, kad trapus

vaikas, dar tik turintis įžengti į paauglystės amžių, neatrodo panašus į bombų „Tamilų tigrams“* gamintoją.

Mažasis Renu buvo įpratęs prie panašių neramumų. Jie nužymėjo jo gyvenimą nuo pat ankstyvos vaikystės. Prieš penkerius metus, 1983 m. liepą, kai jam buvo tik šešeri, su šeima jis buvo evakuotas iš Kolombo. Tamilų kovotojai buvo nužudę trylika Šri Lankos kariuomenės kareivių. Atsikeršydama sinhalų** minia sostinėje Kolombe išskerdė šimtus nekaltų tamilų ir taip sukėlė ilgalaikį pilietinį karą, – šis baigėsi tik po dvidešimt šešerių metų.

Gyventi nuolatiniame pavojuje Kolombe, kai visame mieste plėšikauja sinhalų gaujos, nebuvo išmintinga, taigi Renu tėvai susikrovė daiktus ir su trimis savo vaikais išvažiavo į Džafną, pagrindinį Šri Lankos tamilų bendruomenės centrą. Šiaurinėje šalies dalyje esančią Džafną nuo pietrytinės Indijos pakrantės skiria tik penkiasdešimt kilometrų. Miestas buvo tamilų partizanų citadelė. Pasipriešinimas Kolombo vyriausybei, kurios daugumą sudarė sinhalai, nuolat augo.

Neilgai trukus po Renu persikėlimo, neprognozuojami pilietinio karo žiaurumai ir maištai vis labiau artėjo prie jo naujųjų namų. 1987 m. vyriausybinės kariuomenės pajėgos apgulė Džafną, kovodamos su įvairiomis ginkluotomis grupuotėmis, ypač su liūdnai pagarsėjusiais „Tamilų tigrais“. Skaičius pabėgėlių, srūvančių iš miesto į pietinę Indiją, tapo kritinis, o tai įtikino Naujojo Delio vyriausybę imtis veiksmų. Pagal susitarimą su Šri Lankos vyriausybe indai pasiuntė didžiules taikos palaikymo pajėgas į Džafną prižiūrėti taikos sutarties vykdymo.

Tačiau taikos palaikytojams indams nepavyko suvaldyti „Tamilų tigrų“ ir greitai Džafna dar sykį virto vienu iš pavojingiausių miestų žemėje. 1987 m. spalį indų kariuomenės būriai iššudė daug

* „Tamilų tigrai“ – separatistinė kovotojų organizacija, įsteigta šiaurinėje Šri Lankoje, siekusi įkurti nepriklausomą tamilų valstybę Tamil Elamą.

** Sinhalai – didžiausia Šri Lankos etninė grupė.

nekaltų civilių pagrindinėje miesto ligoninėje, ir tai buvo vienintelis įvykis per ketvirtį amžiaus trukusį pilietinį karą, kuris vienodai papiktino ir Kolombo vyriausybę, ir „Tamilų tigrus“. Renu ir jo šeimai pasilikti Džafnoje tapo per daug pavojinga, taigi jie parkeliavo ilgą kelią atgal į pietus, į Kolombą.

Vieną popietę Renu tėvas paprašė mažąjį berniuką parnešti kai ką iš maisto parduotuvės. Renu, dar niekada nematęs tiek daug rupijų, susikišo jas į kišenę kartu su sąrašu prekių, kurias turėjo nupirkti. Eidamas į parduotuvę, pakelėje jis pastebėjo vyriškį, žaidžiantį kažkokį žaidimą. Vyriškis turėjo tris puodus, o viename iš jų buvo padėtas akmenukas. Renu stebėjo, kaip miklus pokštininkas žaibišku greičiu perstato puodus, o tada žmonės deda pinigus prieš vieną ar kitą puodą. Renu buvo pakerėtas ir nustebintas, kad žaidėjams amžinai nepavyksta atspėti, kur yra akmenukas, o jis kas kartą atspėdavo teisingai. Renu prasibrovė į eilės priekį ir išsitraukė suglamžytus tėvo banknotus. Vieną po kito vyriškis susikišo juos į kišenę, nes Renu nesugebėdavo atspėti puodo su akmenėliu lygiai taip, kaip ir tie, kurie tai darė prieš jį. Vis dėlto kuo daugiau pralošdavo, tuo su didesniu įkarščiu jis lažindamasis statė pinigus. Nekreipdamas dėmesio į pralaimėjimus, jis tiesiog negalėjo sustoti tol, kol nebeliko banknotų, o jo mažą kūnelį, apsvaigusį nuo adrenalino, staiga išpylė šaltas prakaitas, įsivaizdavus aukštai virš galvos iškeltą tėvo ranką. Daugiau jis niekada nebesilažino.

Per kelerius metus, prabėgusius nuo tada, kai jie išvyko iš Džafnos, sostinė šiek tiek aprimo, nors jos gyventojai tamilai niekada nesijautė visai saugūs, – tą įrodo ir kariškių reidas į jų namus. Renu šeimai liko vienintelė išeitis – bėgti.

Dar nesulaukusiam paauglystės Renu ne kartą svilo padai, sprunkant nuo vienos pavojingos situacijos ir pakliūvant į dar pavojingesnę, o kartais jam tiesiogine prasme pavykdavo išvengti kryžminės ugnies. Netrukus po kariuomenės reido į jų namus, kai

dėl įgimtos žymės odoje berniukas vos nebuvo palaikytas teroristu, Renu močiutė nusprendė, kad jo, kaip prie pilnametystės artėjančio tamilo, padėtis Šri Lankos sostinėje yra per daug rizikinga. Jis gali susigundyti prisidėti prie „Tamilų tigrų" arba užrūstinti po sostinę šmižinėjančias nacionalistines sinhalų grupes. 1992 m. šeima sukrapštė pakankamai pinigų, kad galėtų išsiųsti Renu į Londoną, kur gyveno jo teta ir dėdė.

Naujasis gyvenimas kitame pasaulio krašte, visiškai nepažįstamoje aplinkoje, turėjo savų pavojų. Langdono mokykloje – vienoje iš didžiausių ir maištingiausių rytų Londone – mažas ir plonas kaip šakaliukas Renu atsidūrė tarp dviejų didelių bendruomenių: baltųjų ir bengalų. Jam gerai sekėsi matematika – čia jis pralenkė visus bendraamžius, bet buvo labai sunku reikšti mintis anglų kalba. Negailestingai ujamas kaip visiškas nepritapėlis, po šešių mėnesių Renu paprasčiausiai atsisakė lankyti mokyklą, kad ir kaip beviltiškai maldavo teta ir dėdė.

Dvejus metus Renu praleido užsidaręs namuose, kartais ištisas savaites neišlįsdamas į gryną orą. Vienintelis jo užsiėmimas buvo nuo ryto iki vakaro žiūrėti televizorių.

Renukanthas Subramaniamas išmoko būti vienas.

Ir galbūt taip ir būtų likęs vienas, jei galiausiai dėdė nebūtų privertęs jo išlįsti iš namų ir pradėti mokytis Niuamo tolesnio švietimo koledže. Čia Renu įgijo kai kurių naujų įgūdžių: bendrauti su bendraamžiais, rūkyti marihuaną, gerti brendį „Martell" ir programuoti kompiuterį.

Vietiniame alaus bare, girtutėlis ir apsvaigęs nuo narkotikų, Renu triuškindavo žaidimų automato „Gatvės kovotojas" virtualius oponentus.

Kiek jaunų žmonių buvo liguistai įsitraukę į šias hipnotizuojančias dvikovas, kuriose jų avatara metamas į mirtiną kovą prieš minias tokių pat agresyvių kovotojų? Ar tai tramdė jų agresyvumą,

ar jį skatino? Ar dopamino antplūdis priekinėje smegenų skiltyje, kurią sužadina šie žaidimai, sukelia intensyvų potraukį visiems jauniems žmonėms, ar tik kai kuriems iš jų?

Renu trankydavo automatą ir taip pripildydavo savo organizmą adrenalino, o smegenis – endorfinų. Baigęs, vis dar įsiaudrinęs ir norėdamas išlaikyti gerą savijautą ir apsiraminti, jis griebdavosi brendžio „Martell“. Dėl šio dvigubo įpročio menki jo išlaikymui skirti pinigai palengva tirpo. „Gatvės kovotojas“ jo gyvenime darėsi vis svarbesnis. Atsigulus į lovą, mintyse atgydavo ryškūs smurtiniai žaidimo vaizdai.

Tačiau kaip kažkada nustojo lažintis, taip dabar Renu apsisprendė liautis žaidęs ir daugiau niekada nebepalietė automato. Nelaimei, tuo metu apsisprendė tik dėl „Gatvės kovotojo“, bet ne dėl augančio gėrimų ir narkotikų pomėgio.

Tai, kad nustojo žaisti žaidimus, dar nereiškė, kad jis apskritai prarado aistrą kompiuteriams. Jis pamilo juos nuo tada, kai, būdamas devynerių ir dar tebegyvendamas Šri Lankoje, pirmą sykį pabandė žaisti kompiuteriu. Kadangi amžinai trūko pinigų, jis niekada negalėjo naudotis kompiuteriu nuolatos, bet, peržengęs dvidešimtuosius metus, įveikė šią problemą, nutaręs studijuoti kompiuterių mokslus Londono Vestminsterio universitete.

Netrukus Renu atrado vadinamąsias *warez* – piratines programas, kurios, įsilaužus į jų apsaugos sistemas, buvo išplatintos tarp kompiuterių entuziastų, bendru vardu vadinamų Scena.

Tai buvo pasaulis, kuriame jis tuo pat metu galėjo būti ir su draugais, ir vienas.

10
Žaidimų teorija

Eislingenas, Badenas-Viurtenbergas, 2001 metai

Kaip tik tuo metu, kai Renu pirmą kartą tyrinėjo Sceną, už 500 mylių, pietų Vokietijoje, tą pačią paslaptingą bendruomenę užtiko kitas jaunas kompiuterininkas.

Penkiolikmetis Matrix001 įsimylėjo. Bet ne merginą. Jis pametė galvą dėl kompiuterinių žaidimų. Iš pradžių tai buvo tik vienas iš jo harmoningos ir normalios paauglystės užsiėmimų, kuriam jis skirdavo savo laisvalaikį, kaip ir sportui bei mokyklos orkestrui, kuriame grojo klarnetu. Iš pažiūros vaikinas neatrodė kuo nors ypatingas. Savo slaptą aistrą žaidimams jis lengvai nuslėpdavo. Niekas to nežinojo – nei draugai, nei tėvai ar broliai ir seserys – nebent jo jaunesnis broliukas.

Jis ne tik dievino žaidimus, bet ir buvo labai įgudęs, o artėjant baigiamiesiems mokyklos egzaminams ligi gilios nakties užsisėdėdavo prie kompiuterio. Koja kojon suspėti su naujausiais žaidimais buvo brangu, o garbinami buvo tie, kurie galėjo paskelbti, kad jau žaidė ką tik pasirodžiusius naujus žaidimus ir tapo nugalėtojais (o kaip tik taip ir buvo tarp Matricos žaidimų draugužių).

2000-aisiais į rinką pasipylė nauji žaidimai su nuostabia grafika. Greitai ir gausiai buvo prigaminta „Pokemonų“ serijų ir dar ekstremalesnių žaidimų, tokių kaip didelio populiarumo sulaukusios videožaidimų serijos „WWF Smackdown! 2: Know Your Role“ ir „Grand Theft Auto“, kurių siužetinės linijos pasižymėjo žiauriomis scenomis

ir pornografiniais elementais. Matrica visada troško išbandyti naujausius žaidimus, bet jų visų turėti jis paprasčiausiai neįstengė.

Kalbant apie žaidimus, jo ir Renu gyvenimai nesiskyrė, bet daugiau šiuodu jaunuoliai neturėjo nieko bendro.

Nusprendęs patenkinti jį užvaldžiusią aistrą, Matrica atrado internetinę bendruomenę, vadinamą „fXp scena". Tai buvo svarbus momentas ne tik Matricos gyvenime, bet ir visoje greitai besikeičiančioje internetinėje kultūroje.

Per du dešimtmečius nuo atsiradimo asmeniniai kompiuteriai tapo aistringų, o kartais ir slaptų diskusijų apie jų vaidmenį visuomenėje tema. Diskusijose dalyvavo kompiuterių kūrėjai, šalininkai ir labiausiai atsidavę naudotojai. Filosofiniuose debatuose iš esmės išsiskyrus nuomonėms apie interneto reikšmę, daug internetinių įgūdžių buvo priskirta prie nusikalstamų.

Paprastai tariant, debatai vyksta tarp tų, kurie tiki, kad svarbiausias yra interneto komercinis vaidmuo, ir tarp tų, kurie teigia, kad visų pirma tai yra socialinė ir intelektinė priemonė, kurios pati prigimtis keičia esminius masinių komunikacijų moralinius principus. Pirmieji bet kokį aiškiai nesankcionuotą programavimo simbolių, vadinamųjų „kodų", kopijavimą laiko kriminaliniu nusižengimu. Antrieji yra įsitikinę, kad perleidžiant ar platinant programinę įrangą taip pat yra perleidžiamos ir autoriaus teisės.

Klausimo esmė atsiskleide jau seniai, dar 1976 m. vasario mėnesį, kai Billas Gatesas atviru laišku kreipėsi į mėgėjus – dar tik besiformuojantį kompiuterių naudotojų būrį, iš kurių ateityje išaugs kompiuterių fanatikai, programišiai ir įsilaužėliai į sistemas. Tame laiške Gatesas apgailestavo, kad 90 procentų tų, kurie naudojasi pirmąja „Microsoft" paketo programavimo kalba „Altair Basic", jos nepirko. Jie paprasčiausiai ją nusikopijavo. O tai reiškia, kad Gatesas negavo pelno iš įdėto milžiniško masto darbo ir iš tų pinigų, kuriuos investavo į šios programavimo kalbos sukūrimą. Nors Gateso

kalba nebuvo itin elegantiška, kaip būdinga daugeliui kompiuterių fanatikų, jo išsakyta mintis buvo aiški: mėgėjus jis kaltino vagyste.

Mėgėjai, fanatikai ir programišiai, kurie vėliau imti vadinti įsilaužėliais, su tuo nesutiko. Jų nuomone, nuo tada, kai „kodai" pasidarė prieinami, naudotis jais buvo sąžininga. Tiek Vakarų pakrantėje, tiek Masačusetso technologijų universitete Kembridže kai kurie svarbiausi kompiuterių kūrėjai ir pirmieji jų naudotojai buvo smarkiai užsikrėtę „kumbaya"* ideologija, pagal kurią buvo teigiama, kad ši ypatinga technologija padeda pasauliui susivienyti ir dėl tam tikros, nors ir neišreikštos priežasties nėra pavaldi toms autorių teisių normoms, kurios tradiciškai taikomos knygoms, muzikai ir kitai kūrybai.

Visiškai suprantama, kodėl taip galėjo atsitikti: anksčiau buvo neįmanoma atspausdinti ir padauginti nelicencijuotų knygų ar padaryti ilgai grojančių plokštelių kopijų, nes nebuvo reikalingų prietaisų. O jei kas juos ir turėjo, šie prietaisai buvo griozdiški, stacionarūs, ir teisėsaugai, ginančiai intelektines autorių teises, buvo lengva juos susekti.

Programavimo simboliai („kodai") ar programinė įranga buvo visai kas kita. Nuo kasetinių įrenginių, į kuriuos būdavo įrašomi pirmieji devintajame dešimtmetyje sukurti privačiam naudojimui skirti kompiuteriniai žaidimai, pereita prie diskelių, kompaktinių, universaliųjų skaitmeninių ir standžiųjų diskų. Tuo metu komercinės kompiuterinės įrangos gamintojų imperija pabandė suduoti pirmąjį atsakomąjį smūgį ir suteikė savo gaminiams papildomus kodus, kurie turėjo apsaugoti nuo neleistino jų kopijavimo. Kompaktiniai diskai ir kasetės paprastai turėdavo skaitmeninius „užraktus".

* „Kumbaya" arba „Kumbayah" – afroamerikiečių religinė giesmė, kuri šiais laikais siejama su žmonijos vienybės ir dvasingumo, artumo ir gailestingumo idėjomis.

Ši suprantama taktika netikėtai davė priešingą rezultatą. Dar 1982 m. kitas vokiečių paauglys, vėliau tapęs paslaptinguoju programišiumi pravarde MiCe!, galiausiai įtikino savo tėvus – geriau jau būtų buvę priešingai – Kalėdų proga nupirkti jam kompiuterį. Tačiau, išleidę visus kompiuteriui skirtus pinigus, jie nesutiko duoti jam nė pfenigo žaidimams, nes nesuvokė, kad be žaidimų programinės įrangos, kuri tuo metu buvo įrašoma į kasetes ir labiausiai rūpėjo jų sūnui, kompiuteris jam nereikalingas.

Vaikinas sumojo, kad norint naudotis kompiuteriu jam lieka vienintelė išeitis – pasiskolinti programas iš draugų, o tada nusikopijuoti. Pasitaikius tokiai progai, jis išsiaiškino, kad kasečių nukopijuoti negalima. Jis išbandė viską, kas įmanoma, bet kas kartą tik sugadindavo kompiuterį. Po ilgų nusivylimo dienų ir naktų galiausiai tam tikroje juostelės vietoje jis pastebėjo kažkokį kodą, kuris neturėjo aiškios funkcijos. Ir tada jam į galvą toptelėjo mintis: šis kodas ir blokuoja kopijavimo procesą! Sykį tai supratęs, MiCe! galėjo eksperimentuoti, perrašinėdamas šį kodą kas kartą kita eilės tvarka, kol vieną vakarą – valio! – jam pavyko jį „nulaužti".

Pirmuosius žaidimų mėgėjus, panašius į MiCe!, įsilaužti pro užblokavimą skatino jų aistra žaidimams, o ne noras užsidirbti pinigų. Vienas žaidėjas perduodavo kopijas kitam. Taip gimė Scena.

Tai vis dar buvo daug pastangų ir laiko reikalaujantis procesas, nes reikėjo fiziškai nukopijuoti kodą į naują kasetę. Nepaisydami to žaidimų mėgėjai su įkarščiu priėmė iššūkį, kurį jiems metė programinės įrangos gamintojai, ir netrukus suklestėjo žymios įsilaužėlių grupės. Vienintelis šios subkultūros tikslas buvo įsilaužti į žaidimus ir kitas programas vos tik joms pasirodžius rinkoje, o tada šiuos sugebėjimus pademonstruoti bendraamžiams.

Taip susikūrė kibernetinis pogrindinis pasaulis, kuris greitai pradėjo skilti į labai skirtingas bendruomenes – ir geras, ir blogas.

11
Kelio atgal nėra

Praėjus beveik dviem dešimtmečiams po to, kai MiCe! įsilaužė į savo pirmąją kasetę, jaunasis Matrica susidūrė su tokia pat dilema. Jį labai traukė žaidimai, bet vaikinas negalėjo jų sau leisti. Dilema buvo ta pati, o technologijos buvo pažengusios tiek, kad tapo beveik neatpažįstamos. Dabar žaidimai pasižymėjo kvapą gniaužiančia įmantria grafika, painiomis siužetinėmis linijomis ir sudėtingais iššūkiais protui.

Daugelio mėgėjų aistra žaidimams taip pat atitinkamai intensyvėjo. Kasetės ir diskeliai jau tapo muziejiniais eksponatais, laikas artėjo prie pabaigos ir CD bei pastoviosios atminties kompaktiniams diskams (CD-ROM)*, DVD ir atminties kortelėms. Vis daugiau žaidimų egzistavo kaip paprasčiausios internetinės programos. Tačiau labai daug jų išsaugoti savo namuose esančiuose asmeniniuose kompiuteriuose buvo neįmanoma. Dar daugiau, tai buvo telefoninių modemų laikai, kai, prisijungus prie interneto, valandų valandas būdavo užimamos telefonų linijos. Bet tie, kurie iš savo namų kompiuterio turėjo prieigą prie daug galingesnio kompiuterio, galėjo išsaugoti visus jiems patinkančius žaidimus ir jais dalytis...

Santrumpa „fXp“ reiškia Failų apsikeitimo protokolą, bet šiaip jau apie „fXp“ užtenka žinoti tik tiek, kad jis įgalina labai greitą

* CD-ROM (angl. *Compact Disc Read-only memory*) – kompaktinis diskas, skirtas tik duomenims saugoti ir nuskaityti, bet ne įrašyti iš kompiuterio. Jis plačiai naudojamas programinei įrangai, taip pat ir videožaidimams, saugoti ir platinti.

duomenų perdavimą iš vieno kompiuterio į kitą. Tai ypač naudinga, keičiantis duomenimis tarp serverių. Svarbu suprasti, kad serveris yra paprasčiausias kompiuteris, pritaikytas funkcionuoti kaip komunikacijų centras. Taigi kokia nors didelė kompanija gali turėti nuosavą serverį, suteikiantį prieigą prie interneto visiems savo darbuotojams. Daugelis serverių yra dideli ir galingi ir jų internetinės prieigos nepriklauso nuo telefono linijų.

„fXp" interneto forumai vienijo bendraminčių kompaniją, kurios nariai įsilaužd avo į serverius, o tada naudodavosi jais žaidimams žaisti ir jiems išsaugoti. Matrica buvo gabus mokinys, taigi greitai jo kompiuteris jau atidžiai tyrinėjo internetą, ieškodamas serverių.

Naudodamasis automatine programa, iš savo kompiuterio į internetą jis išsiųsdavo nesuskaičiuojamą daugybę pranešimų, kurie pasiekdavo bet kurioje pasaulio vietoje esančius serverius ir „pasibelsdavo į jų duris". Kai serveris „atidarydavo duris", Matricos kompiuteris paklausdavo: „Ar galiu užeiti?" Dauguma serverių tada jo kompiuteriui atsakydavo: „O koks slaptažodis?" Bet jis rado pakankamą skaičių tokių serverių, kurių administratoriai nesivargino įsivesti slaptažodžių, taigi tokiais atvejais serveris atsakydavo Matricos kompiuteriui: „Žinoma, prašom užeiti. Aš pasiruošęs padaryti tai, ko panorėsi, tu išdykęs pagrindinis kompiuteri!"

Administratoriai, kurie palikdavo savo kompiuterius šitaip pažeidžiamus, Matricos supratimu, buvo neverti net paniekos. Bet kas galėjo į juos patekti ir pavogti kompanijos paslaptis. Jo manymu, tai niekuo nesiskyrė nuo to, jei, tarkim, pasiėmęs pinigų prikimštą piniginę, ateitum į prekybos centrą, o paskui padėtum ją vidury parduotuvės ir išeitum.

Buvo ir tokių serverių, kurių slaptažodžius buvo lengva atspėti. Pavyzdžiui, kai kurie palikdavo gamintojo slaptažodį, paprastai ką nors panašaus į „admin", arba – patį kvailiausią, kokį tik galima sugalvoti – „slaptažodis".

Kituose kompiuteriuose jis nustatė apsaugos sistemų silpnąsias vietas (galbūt mažai naudojamą jungtį ar prievadą, kuris nepareikalauja slaptažodžio) ir jomis pasinaudodavo, kad prisikastų iki vidinių serverio klodų. Daugumai kompiuterių naudotojų tai galėjo atrodyti panašu į mokslą apie raketas, bet Matricai tai buvo tas pats, kas atidaryti neužrakintas duris. Jis per pusvalandį galėjo bet kurį pamokyti, kaip tai padaryti.

Pirmoji užduotis, kurios Matricai tekdavo imtis, perėmus serverio kontrolę, – tai ištaisyti tą silpnąją vietą, kuria pats pasinaudojo, norėdamas gauti prieigą. Jis turėjo užtikrinti, kad niekas kitas negalės atakuoti serverio taip, kaip jis pats tai ką tik padarė.

Sykį patekęs į serverį, jis jau galėjo jį kontroliuoti. Jei norėjo, galėjo stebėti visą ateinančių ir išeinančių elektroninių žinučių ir interneto „judėjimą". Bet jam tai nebuvo svarbu. Jam rūpėjo tik panaudoti šiuos serverius žaidimams parsisiųsti, išsaugoti ir paskirstyti, naudojantis „fXp" technologija.

Matricai buvo tik penkiolika, bet užsigeidęs jis galėjo pasiekti milžiniškus interneto klodus, apie kurių egzistavimą dauguma suaugusiųjų net nenumanė. Jo tėvai nė nenutuokė apie tą slaptąjį pasaulį, kurį jis tyrinėjo, sėdėdamas savo miegamajame. O jie ir netroško to žinoti – žaidimų ir programų parsisiuntimas buvo aiškiai nelegalus ir pažeidė autorių teises, bet tuo metu tuo užsiėmė tik labai nedidelis naudotojų ratas. Gamintojus tai pykdė, bet nebuvo pragaištinga problema. Daugybė žaidimų buvo puikiausiai perkami legaliai parduotuvėse arba per tokias interneto svetaines kaip „Amazon".

Matrica slėpė savo veiklą nuo tėvų ne dėl to, kad būtų manęs, jog pažeidžia intelektinės nuosavybės teises. Ne – kalbant apie paauglius ir internetą, nuostabiausias dalykas, jų manymu, buvo tai, kad tėvai neturi nė mažiausio supratimo (o daugeliu atvejų niekada ir negalėjo turėti) apie tai, ką jie daro. Tėvams buvo gana sunku atsekti, kokie DVD atnešami į namus ar iš jų išnešami. Bet DVD bent jau buvo

apčiuopiami daiktai, kuriuos mama ar tėtis galėjo atimti, radę savo trylikametį žiūrint tik suaugusiesiems skirtą filmą (be abejo, visuomet rizikuodami išprovokuoti staigaus pykčio priepuolį).

Dėl interneto visa tai keitėsi. Vaikai augo kibernetinėje aplinkoje, kuri jiems buvo savaime suprantama ir normali ir kuri vis labiau glumino jų tėvus, nes jiems darėsi vis sunkiau joje susigaudyti. Paaugliai puikiai suprato, kad tėvai nardo toje pačioje kibernetinėje jūroje. Tai savo ruožtu stiprino pojūtį, kad internetas yra jaunų žmonių sritis, iš kurios tėvus reikėtų ištremti. Argi mažai mamų ir tėčių yra įėję į kambarį ir pastebėję, kaip jų paaugliai vaikai paslepia interneto naršyklės langą, o jų skruostai trumpam parausta? O jei tėvai tik užmeta akį į „Facebook" puslapį, net jei jų atžalos jį atsidaro viešoje patalpoje, vaikai virsta aktyviais žmogaus teisių gynėjais, kaltina tėvus persekiojimu ir elgesiu, panašiu į gestapo karininkų.

Nors daugelis vaikų ir paauglių sugebėjo apdumti akis savo tėvams, tačiau buvo ir kitų suaugusiųjų, kuriuos apgauti nebuvo taip lengva ir kurių gretos vis augo. Prie tokių būtų galima priskirti prievartautojus, įvairius reklamuotojus, priekabiautojus ar sąvadautojus, policininkus, mokytojus ir nusikaltėlius. Juk tik labiausiai išprusę kompiuterininkai sugeba užmaskuoti savo tikruosius veiksmus internete.

Kitaip nei ilgai kentę tėvai, kitos suinteresuotos grupės, turinčios kompiuterinio raštingumo pradmenis, pradėjo atsekti per kelerius metus internete paauglių paliktus skaitmeninius pėdsakus. Šiuose įrašuose jie paprastai rasdavo kvietimų ar sutikimų dalyvauti išgertuvėse, kur neretai vartojami ir narkotikai, mokytojų įžeidinėjimų, priekabiavimų prie klasės draugų ir vis dažniau – internete skelbiamų pornografinių autoportretų. Tėvai gal ir nieko apie tai nenutuokė, bet buvo žmonių, kurie suprato. Net ir tokiems sumaniems vaikams kaip Matrica pernelyg savim pasitikėti buvo neatsargu.

Užvaldydamas prastai apsaugotus serverius, o tada juose išsaugodamas žaidimus ir juos žaisdamas, Matrica iš tiesų nedarė nieko blogo. Pereinamuoju į naują tūkstantmetį laikotarpiu Vokietijoje tai nebuvo laikoma nusikaltimu, o autorių teisės skaitmeniniame amžiuje buvo apibrėžtos miglotai. Paaugliai ir jaunuoliai pradėjo keistis muzikiniais failais, naudodamiesi interneto svetainių „Audiogalaxy" ir „Napster" paslaugomis. Norėdami per šias svetaines parsisiųsti, tarkim, „Queen" grupės kūrinį „Bohemiška rapsodija" (*Bohemian Rhapsody*), jūs galite būti nukreiptas į kažkur, gal kitame pasaulio krašte, esantį kitą kompiuterį, kuriame ši daina yra išsaugota. Pasinaudodamas svetaine tarsi tiltu, galite parsisiųsti šios dainos kopiją į savo kompiuterį.

Per labai trumpą laiką milijonai žmonių suprato, kad jiems nebereikia pirkti muzikinių įrašų – viską galima gauti nemokamai! Apsikeitimas failais sudarė šiokių tokių nepatogumų kompiuterinių žaidimų verslui, tačiau muzikos pramonei tai buvo didžiulis iššūkis. Bandant įveikti šią problemą, būtų reikėję, kad teisininkai iš naujo apibrėžtų skaitmeninio amžiaus autorių teises. Paskui reikėtų įtikinti įstatymų leidėjus, kad jie priimtų atitinkamus įstatymus, ir galiausiai reikėtų įtikinti policininkus, kad sulaikyti skaitmeninius piratus yra jų pareiga. Dar daugiau – muzikos verslui tektų sukurti naujas technines apsaugos nuo piratavimo priemones (o to padaryti jiems lig šiol aiškiai nepavyko).

Įprotis dalytis muzikiniais failais – mažais ir lengvai perduodamais iš vieno kompiuterio į kitą, pasklido žaibo greitumu. Muzikos įrašų pardavimas Jungtinėse Valstijose pasiekė viršūnę 1999 m. ir sudarė daugiau kaip 14,5 milijardų dolerių, tačiau jau kitais metais šie skaičiai pradėjo mažėti ir nuo tada tik mažėja.

Priešingai, neteisėtas žaidimų parsisiuntimas, kurį sunkiau įvaldyti, tik šiek tiek sumažino metai iš metų augantį CD-ROM ir DVD pardavimą. Iš tiesų žaidimų platinimas netgi padėjo juos rek-

lamuoti. Taigi blogiausia, ką galima pasakyti apie Matricos kompiuterinius užsiėmimus, yra tai, kad jie neleido jam išsimiegoti ir trukdė atlikti namų darbus.

Visgi Matrica, pats to beveik nepastebėdamas, žengė mažą žingsnelį piktadarybių link.

Internetą atrado ir reklamos pramonė ir, kaip ir visi kiti, mėgino sugalvoti, kaip geriausiai juo pasinaudoti. Reklamuotojams internetas siūlė išskirtinių pranašumų: visų pirma buvo galima daug tiksliau pasiekti potencialią auditoriją. Norėdami parduoti naujagimių vystyklus, tiesiog turite palikti ramybėje tas svetaines, kurios aptarnauja parašiutininkus, ir atkreipti dėmesį į jauniems tėveliams skirtus interneto forumus. O kai mokate už reklamas per televiziją, radiją ar skelbimų lentose, jos vis tiek pasiekia ir parašiutininkus (gerai, jei šie taip pat yra ir jauni tėveliai).

Antra, galima patikrinti reklamos sėkmę ir sąnaudas. Kas kartą, kai jauna mamytė ar jaunas tėvelis pele spragteli ant vystyklų reklamos, tai užregistruojama, ir rezultatą mato tiek gamintojas, tiek reklamuotojas. Reklamos firmai sumokama pagal šių spragtelėjimų skaičių. Tada reklamuotojai ir pardavėjai gali išanalizuoti vadinamąjį spragtelėjimų dažnį, arba CTR (angl. *click through rate*), taigi vystyklų gamintojas gali pamatyti, tarkim, kad iš 100 parašiutininkams skirtos svetainės lankytojų nė vienas nespragtelėjo ant vystyklų reklamos. Bet dešimt iš šimto jaunųjų tėvelių forumo dalyvių spragtelėjo ant šios reklamos, o tai sudaro dešimties procentų CTR. Reklamos firma gaus atitinkamą užmokestį. O netrukus iš CTR išsivystė ir spragtelėjimų klastojimas.

Vieno forumo, kuriame apsilankė Matrica, administratorius užsiiminėjo internetinėmis suktybėmis. Jis įkalbėjo Matricą pasinaudoti jo kontroliuojamais serveriais ir sukurti programą, kuri tam tikrais vienodais intervalais automatiškai spragtelėtų ant reklaminių skelbimų. Kas kartą, kai taip atsitikdavo, Matrica užsidirbdavo vieną

centą. Jis net ir nesuprato, kad tai nelegalu. Paskui administratorius jam pasakė, kad egzistuoja kitas forumas, kuriame aptariamos panašios temos ir į kurį jam būtų verta atkreipti dėmesį. Tai buvo „CarderPlanet“, kur Matrica pirmą sykį išgirdo apie sukčiavimus su kreditinėmis kortelėmis.

Matrica peržengė Rubikoną apimtas psichologinio transo, nesugebėdamas susivokti aplink jį sūkuriuojančiuose vandenyse. Jis buvo dar vaikas, bet palengva klimpo į nusikaltimų liūną. Kažkuria sąmonės dalelyte gal ir suvokė, kad čia kažkas negerai, bet ribos tarp gėrio ir blogio kibernetinėje erdvėje yra labai miglotos, jei apskritai galima jas įžvelgti.

12
Kelionė į Indiją

Čenajus, Tamil Nadu*, 2001 metai

Atėjus 2001-iesiems, Renu jau devynerius metus nebuvo matęs nei savo tėvų, nei brolių ar seserų. Visgi net ir tokie jauni vyrai kaip Renu, išmokę išgyventi, turėdami labai silpnus ryšius su šeima, retkarčiais privalo atsiliepti į motinos maldavimus. Po ilgų jos prašymų jis pažadėjo, kad atras lėšų skrydžiui į Indijos pietuose esantį Tamil Nadu ir aplankys šeimą ir visus gimines.

Tačiau lėšų surinkti buvo sunku. Studijuodamas Vestminsterio universitete, Renu tuo pat metu dirbo picerijoje „Pizza Hut" ir pristatydavo į namus picas. Jis dirbdavo maždaug iki vidurnakčio ar pirmos valandos nakties, o rytais turėjo anksti keltis, kad spėtų į pirmą paskaitą (nors jo punktualumas bėgant metams nuolat prastėjo). Pirmą sykį gyvenime jis užsidirbo šiek tiek papildomų pinigų. Bet jų nepakako, kad būtų galima susitaupyti: atliekamus pinigus surydavo jo polinkis į kvaišalus – dabar jis jau vartojo kokainą, o netrukus įniko ir į labiausiai žmogų niokojantį narkotiką – iš kokaino išgaunamą kreką.

Nepajėgdamas susitaupyti pinigų bilietui, Renu pasiskolino jų iš draugų, saugumo dėlei už 3 000 svarų nusipirko „American Express" kelionės čekių ir išsiruošė ilgam skrydžiui į Čenajų.

* Čenajus (žinomesnis buvusiu pavadinimu – Madrasas) – uostamiestis pietryčių Indijoje, Bengalijos įlankos pakrantėje, Tamil Nadu – valstija pietinėje Indijos dalyje, kurioje gyvena tamilų tauta.

Niekas nenumanė, ko tikėtis iš susitikimo, – Renu paliko motiną dar būdamas vaikas. Dabar jis buvo jau beveik suaugęs jaunuolis, kurio gyvenimas buvo nužymėtas intensyvios vienatvės tarpsnių. Palyginti su koledžo laikais, jis daugiau bendravo, vis dėlto jam sunkiai sekėsi palaikyti nerūpestingą pokalbį, o ir emocijų reikšti nelabai mokėjo.

Kelionė prasidėjo nesėkmingai. Iš Čenajaus į kaimą teko važiuoti sausakimšu šaltu indišku autobusu kartu su daugybe žmonių, vištų ir begale bagažo. Pusiaukelėje, mieguistas po ilgo skrydžio iš Londono, jis pajuto lengvą truktelėjimą ir akimirksniu prasiblaivė. Nieko blogo nepagalvojo, bet susitikimo su motina džiaugsmą aptemdė tai, kad išlipęs iš autobuso pastebėjo, jog jo maža rankinė prapjauta, o 3 000 svarų vertės kelionės čekiai ištraukti.

Bet jo laukė dar blogesni dalykai. Apsilankius „Amex"* kontoroje Čenajuje, darbuotojai atsisakė jam kompensuoti prarastus čekius (nors, kaip jis manė, čekiai yra saugesni už grynuosius). Norint gauti jų pakaitalus, jam būtų tekę pateikti raštišką vietinės policijos patvirtinimą, kad čekiai dingo. Renu taip pat buvo pasakyta, kad „Amex" negarantuoja pinigų grąžinimo visais atvejais, tačiau gali atlyginti „savo nuožiūra".

Grįžusį į Angliją, „Amex" biurokratai sutiko jį panašiais akmeniniais veidais. Jie išliko nepalenkiami ir teigė, kad Renu nepateikė jiems reikalingų dokumentų, patvirtinančių, jog čekiai buvo pavogti ar pamesti. Jokių išmokų nebus.

Pinigų jis pasiskolino iš draugų. Tačiau viskas turi ribas. Jie užjautė jį, patekusį į keblią padėtį, bet vis tiek norėjo atgauti pinigus. Renu galėjo sumokėti skolą vieninteliu būdu – įsigydamas kreditinių kortelių. Šiaip ar taip, tai buvo jų amžius ir bankai bei kredito kompanijos siekė pritraukti naujų klientų – ar tai būtų Renu, ar bet kas kitas.

* „American Express" – pasaulinė finansinių paslaugų korporacija.

Nepelningas darbas picerijoje negalėjo patenkinti jo augančių finansinių poreikių. Reikėjo pinigų skolai grąžinti, gėrimams ir narkotikams, mokesčiams už mokslą koledže, nuomai. Renu pasaulis pradėjo klibėti. Pirmiausia nukentėjo mokslai. Išlaikęs pirmųjų metų egzaminus Vestminsterio universiteto Harou koledže, jis ėmė vis rečiau ir rečiau rodytis paskaitose ir neišlaikė antro kurso egzaminų ir skolų.

Bėgdamas nuo nevilties, jis liguistai įniko siųstis dainas internetu, naudodamasis muzikos failų apsikeitimo sistema „Napster", o paskui atrado svetaines, kuriose Scenos nariai keitėsi „nulaužtais" žaidimais ir programomis. Naktys dar pailgėjo, kai Renu nugrimzdo į tolimą ir saugų blyksinčių ekranų pasaulį ir pasislėpė nuo jį supančių realybės baisumų.

Vieną vakarą jis pasipasakojo apie prarastus „Amex" pinigus vienam iš daugelio internautų, su kuriais buvo susipažinęs per IRC pokalbių svetainę.

„Pasižiūrėk internete adresu amexsux.com, – patarė jo pokalbių bičiulis, – net jei tai niekuo nepadės, bent jau pasijusi geriau!"

Renu patiko naujoji svetainė ir jos logotipas: „IŠVAŽIUOK iš namų be jų". Čia buvę „American Express" klientai liejo pyktį dėl patirtų nesėkmių. Priešiškumas būtent šiai kompanijai yra gana didelis, tai liudija paieškos per „Google": egzistuoja šimtai svetainių, skirtų nusiskundimams prieš „Amex", ir daugelis pateikia gana įspūdingą skaičių nuorodų į kitas svetaines, skelbiančias naujas bjaurias istorijas, charakterizuojančias kompaniją. Vienas internetinio forumo skelbimas pasiūlė originalią idėją tiems, kurie jautėsi šios kompanijos nuskriausti: „Atkeršykite! Žiūrėkite adresu www. CarderPlanet.com!"

Kai Renu leidosi ieškoti „CarderPlanet", jis pajuto, kad jau pats laikas atsisveikinti su savo asmenybe. Taip jis tapo JiLsi, kurio avatara turėjo piktojo animacinių filmų pirato veidą su raudona skrybėle

ir juodu raiščiu ant kairės akies. Tarsi tikras kibernetinių Karibų kapitonas Džekas Sparou, išmetęs inkarą „CarderPlanet“ pakrantėje, jis greitai pasijuto savas nedorėlių programišių, įsilaužėlių ir sukčių įguloje. Kažkur šioje nepritapėlių prie visuomenės grupėje sukiojosi Matrica, ir nors praėjo dar keli mėnesiai, kol jie apsikeitė virtualios draugystės priesaika, abu tapo žinomomis asmenybėmis, klajojančiomis tarp nesuskaičiuojamos daugybės interneto svetainių, siekiančių kopijuoti „CarderPlanet“.

Kur dar galėtumėte rasti narkomaną pabėgėlį iš Šri Lankos, susidėjusį su griežtų pažiūrų vidurinės klasės vokiečių paaugliu, ir abu susižavėjusius charizmatišku odesiečiu, puoselėjančiu viziją apie naująją Ukrainą? Tiktai internete.

13
Šešėlinė šalis

Niujorkas, Niujorkas, 2003–2004 metai

Raudonoji Brigada (RedBrigade)* nusprendė, kad atėjo laikas smogti „Washington Mutual"** bankui, kuris, jo supratimu, buvo nei daugiau, nei mažiau kaip laisvų pinigų tiekėjas. Iš tiesų bankas jau nuo 1983 m. buvo praradęs *mutual*** statusą, o jo valdytojas buvo paskelbęs, jog šią garbingą instituciją iš Sietlo jis ketina paversti bankininkystės „Wal-Mart"****. Plėšk, kur tik gali, – tokia buvo boso filosofija. Skirstyk paskolas, per daug nesigilindamas į kliento turtą, skolas ir uždarbį. Žarstyk rizikingas būsto paskolas, patraukliai jas pateikdamas. Kuo mažiau investuok į personalą ir įrangą. Tokia buvo pigi bankininkystė be jokių nereikalingų puošmenų. Raudonosios Brigados ir jo bičiulių laimei, nereikalingomis puošmenomis buvo laikomos ir elementarios apsaugos sistemos.

Apie vienuoliktą ryto jis išėjo iš viešbučio „Four seasons", esančio 57-osios ir 5-osios gatvių sankryžoje. Nors buvo dar ne visai išsiblaivęs

* „Raudonosios brigados" buvo marksistinė-leninistinė teroristinė organizacija, įsikūrusi Italijoje. Čia – veikėjo slapyvardis.

** „Washington Mutual, Inc.", sutrumpintai „WaMu", buvo taupomųjų bankų holdingo kompanija ir buvusios „Washington Mutual Bank" – didžiausios Jungtinių Valstijų taupymo ir paskolų asociacijos – savininkė iki jai žlungant 2008 metais.

*** Savitarpio, abipusiai naudingas. (Angl.)

**** „Wal-Mart Stores, Inc." – didžiausias JAV mažmeninės prekybos tinklas pasaulyje.

po vakarykščio lėbavimo, šampanas buvo aukščiausios rūšies, o kokainas beveik grynas, todėl jautėsi visai pasirengęs mūšiui.

Pasiekęs banką, jis atsainiai priėjo prie neįgudusios banko darbuotojos („jiems neverta tiek daug mokėti“) ir ištiesė jai „WaMu“ debetinę kortelę.

– Kiek šiandien norėtumėt, pone?

– Prašyčiau dešimt tūkstančių.

– Puiku!

Tip tap, tip tap. Čia, „WaMu“ banke, Raudonoji Brigada turėjo paduoti savo kortelę banko darbuotojai, kad ši perleistų ją per nuskaitymo įrenginį. Bet kuriame kitame banke tai būtų ta akimirka, kai banko darbuotoja savo ekrane perskaitytų pranešimą, liepiantį „nedelsiant paskambinti“. Raudonajai Brigadai tektų stebėti banko darbuotojos veidą. Ar ji šią akimirką man kažką murma? Gal geriau bėgti? Ar tiesiog stovėti čia kaip kokiam silpnapročiui ir laukti, kol pasirodys policininkai? O gal visgi nėra nieko blogo ir aš tiesiog tampu paranoiku?

„WaMu“ banke nieko panašaus neatsitinka. Tie šykštuoliai pagailėjo pinigų kompiuterių ekranams ir užkoduotiems apsaugos pranešimams. Taigi jei šioje įstaigoje kortelė būtų atmesta, Raudonoji Brigada tiesiog nutaisytų šiek tiek nustebusią miną, atsiprašytų ir išeitų. Niekas iš „WaMu“ nekviestų policijos.

Tačiau jo kortelių niekada neatmesdavo. Tą 2003 m. gruodžio dieną mergina perbraukė jo kortele per prietaisą ir ši iš karto buvo patvirtinta. Tada jis pasirašė išspausdintame kvite, kuriame buvo įrašytas sandorio kodas, ir nuėjo prie bankomato, esančio priešais banką. Įvedė kodą. Akimirką palaukė, o tada, tarsi koks fantastiškas vienarankis banditas iš Las Vegaso kazino, bankomatas pradėjo spjaudyti grynuosius penkiasdešimties dolerių kupiūromis: 1 000, 2 000, 3 000... ir dar, ir dar, kol Raudonoji Brigada į kišenę susikišo du šimtus naujutėlaičių penkiasdešimties dolerių vertės banknotų.

Kartais atrodydavo, kad bankai jam ir jo draugams tyčia paliko atvirus bankomatus. Tai taip paprasta, manė jis, tarsi jie būtų išrinktieji. Jam ypač patiko pumpuoti pinigus iš „Citibank“. Šis bankas labiausiai buvo to nusipelnęs. Pirma, iš visų tų šunsnukių bankininkų jis buvo pats amoraliausias. Antra, jo apsauga buvo visiškai netikusi.

Nuo pat pradžių sukčiavimas, vadinamas „fišingu“ (angl. *phishing*), buvo svarbiausias iš visų kibernetinių nusikaltimų. Net jeigu kompanija turėjo labai tvirtą skaitmeninę apsaugą, ir palyginti ne itin patyręs programišius „fišingo“ ataka galėjo ją pralaužti. Šio metodo esmė – masinis elektroninių žinučių išsiuntinėjimas adresatams, kurie kartais priklauso tam tikrai kompanijai, pavyzdžiui, bankui, o kartais yra parenkami atsitiktinai. Daugelyje šių žinučių būna arba virusu užkrėstas priedas, arba nuoroda, kurią paspaudus interneto naršyklė nukreipiama į tam tikrą svetainę ir ši automatiškai atsiunčia kenkėjišką programą. Jeigu programišius išsiunčia kelis milijonus tokių žinučių, nebūtina, kad į juos sureaguotų daug kompiuterių – tai daryti visais atvejais verta, nes kiekvienas į pavojų pastatytas kompiuteris suteikia prieigą prie banko sąskaitų ir kitos asmeninės ar finansinės informacijos.

Bankai visada susidurdavo su viena didžiule savo klientų saugumo problema (nors tai nepateisina pasibaisėtinai silpnų bankų apsaugos sistemų, egzistavusių pirmuosius penkiolika internetinės bankininkystės metų). Pačios geriausios tinklinės sistemos buvo vertos tik tiek, kiek jų silpniausioji grandis – o mes, šimtai milijonų klientų, buvome atitinkamai pažeidžiami.

Taigi jei bankas yra nepralaužiamas, kibernetinis vagišius prašys jo klientų pagalbos. Tereikia sąskaitų savininkams išsiųsti milijonus elektroninių žinučių, kurios atrodytų tarsi atsiųstos iš jų banko, o tada laukti atsakymų: sąskaitų numeriai ir slaptažodžiai užgrius kaip lavina.

„Citibank“ klientų apgaudinėjimas – nesunkus uždavinys:

Nusipirk daug naujai „nulaužtų“ elektroninio pašto adresų. Patikrink.

Nusipirk „Dark Mailer“* programą, kiekvieno kibernetinio sukčiaus slaptą svajonę. Patikrink.

Nusipirk įgaliotuosius serverius (angl. *proxies*). Patikrink.

Nusipirk prieglobą svetainei patalpinti internete (angl. *hosting*). Patikrink.

Sukurk naują „Citibank“ interneto puslapį. Patikrink.

Įdėk tinklalapyje pasirodantį langelį, kuris neišnyksta tol, kol neįvedamas kortelės numeris ir PIN kodas. Patikrink.

Nurodyk elektroninio pašto adresą, į kurį turės suplaukti sąskaitų numeriai ir slaptažodžiai. Patikrink.

Kiekvieną dieną Raudonoji Brigada dirbo savo suktą darbą. Šį sykį jis žiūrėjo į kažkokios daktarės H. M. Hebeurt iš Niujorko valstijos šiaurinės dalies banko sąskaitos rekvizitus. „Hmmm... ji gyvena netoliese. Po velnių, ji uždirba 50 tūkstančių per mėnesį, o jos suknistas vyras partempia namo daugiau nei 72 tūkstančius!“ Pažvelgęs atidžiau pamatė, kad jo taikinys dirba Volstrite. Galbūt, jei gyvenimas jam būtų suteikęs geresnių šansų, jis būtų galėjęs vogti legaliai, taip, kaip šis vyrukas... Bet jis negalėjo sau leisti nugrimzti į panašias fantazijas, taigi paprasčiausiai pradėjo skaičiuoti. Gerai: dvi einamosios sąskaitos, dvi taupomosios sąskaitos, viena kredituota sąskaita („overdraftas“) ir viena kreditinė kortelė... po 2 000 dolerių iš kiekvienos. Iš viso 12 000 dolerių vienu sykiu.

* Elektroninių žinučių siuntimo dideliais kiekiais programa, užtikrinanti beveik visišką siuntėjo anonimiškumą.

Ir taip kasdien po penkiasdešimt nedidelių žuvelių* įplaukdavo į jo sąskaitą.

Niujorko „Washington Mutual" banke jis šėlo šiek tiek ilgiau nei dvi savaites, o per tą laiką į jo tinklą pakliuvo beveik 300 000 dolerių. Visai neblogai, kadangi jo savaitinės išlaidos sudarė apie 70 000 dolerių. Kas du ar tris mėnesius jis nusipirkdavo naują aukščiausios klasės „Mercedes-Benz" ar „BMW" automobilį. Keliaudavo, savaime aišku, tik pirmąja klase. Jis tiek pat susimąstydavo prieš pirkdamas 10 000 dolerių kainuojantį „Breitling" rankinį laikrodį, kiek mes galbūt susimąstome prieš nusipirkdami laikraštį. Turėjo puikų butą Aukštutiniame Ist Saide, bet jame nakvodavo tik du ar tris kartus per savaitę, nes labai mėgo prabangius miesto viešbučius. Raudonoji Brigada uždirbdavo daugiau pinigų nei Anglijos aukščiausiosios lygos futbolininkas, bet jam nereikėjo mokėti 50 procentų mokesčių.

Jam nebuvo nieko nepasiekiamo. Susiglemžęs penkiasdešimties dolerių vertės banknotus, kasininko veide jis įskaitydavo klausimą: „Kas gi, po galais, yra šis vyrukas?" Jis įsivaizduodavo juos manant, kad jis yra arba iš turtingos šeimos kilęs britas, arba prekiautojas narkotikais. Tačiau kreditinių kortelių amžiuje didžiausi turtuoliai galėjo vilkėti tiek marškinėliais ir džinsais, tiek ir „Savile Row" kostiumais. Šiaip ar taip, komersantai – juvelyrai, prekiautojai automobiliais, vyno pardavėjai, viešbučių savininkai – visada imdavo pinigus neklausinėdami. Banko darbuotojai niekada negalėjo būti tikri: o gal šis nesiskutęs vyrukas yra „Google" savininkas? O ir šiaip – kam rūpi, kaip jis uždirbo pinigus?

Jį erzino tik vienas dalykas. Jis turėjo per daug grynųjų. Vieną vakarą grįžo namo su 77 000 dolerių kišenėje, parėjo į butą, kuriame

* *Phish* ir *phishing* angliškai tariama taip pat kaip *fish* ir *fishing*, o tai reiškia žuvis ir žvejyba.

šen bei ten buvo padėta dar 300 000 dolerių ir 110 000 dolerių vertės piniginių perlaidų. Raudonoji Brigada buvo sumanęs vykdyti grynųjų pinigų paėmimo operacijas pasauliniu mastu, taigi perduodavo kortelių ir sąskaitų duomenis tarpininkui Rytų Europoje, šis organizuodavo bankomatų užpuolimus, o tada siųsdavo grynuosius Raudonajai Brigadai. Šiose operacijose jam vėl tekdavo pačiam užsiimti bankininkyste. Jis pavargo stengdamasis neviršyti Ataskaitų teikimo gairių – bet kuris banko sandoris, viršijantis 10 000 dolerių limitą, remiantis Kovos su pinigų plovimu taisyklėmis, turėjo būti užregistruotas Finansų ministerijoje. „Velniai griebtų, – manė jis, – kas galėjo žinoti, kad atsikratyti pinigais gali būti taip sunku!"

Jam ruošiantis vėl paimti 77 000 dolerių – o tai prilygo paprastam pasivaikščiojimui per kelis kvartalus nuo jo buto – į galvą šovė mintis: „Aš turiu tiek pinigų, kiek niekada nesitikėjau." Jis suprato, kad visas šis reikalas yra labai nešvarus. Bet galvoje nuolatos kirbėjo vienintelė mintis: „CarderPlanet" buvo vienas dalykas, bet kas kada nors galėtų patikėti šita sumauta „Shadowcrew"*? Kas patikėtų, kad diena po dienos aš galiu įeiti į bankus ir kaskart išeiti iš jų su penkiasdešimt tūkstančių kišenėje? Juk tai beprotybė!"

Prieš galutinai žlugdama 2004 m., „CarderPlanet" galėjo pasigirti ne tik internetiniu forumu rusų ir anglų kalbomis, bet ir jau sukurtomis korėjiečių, kinų ir netgi arabų sekcijomis. „CarderPlanet" buvo tikras virsmas, – sakė buvęs FTB specialusis agentas E. J. Hilbertas, kelerius metus tyrinėjęs šią interneto svetainę, – visi „CarderPlanet" pasekėjai šią svetainę laikė modeliu. Neperdėsime pasakę, kad ji paskleidė kriminalinių įsilaužimų praktiką po visą pasaulį."

Atsirado daugybė svetainių, sukurtų pagal „CarderPlanet" pavyzdį: „theftservices.com", „darknet.com", „thegrifters.net", „scan-

* „ShadowCrew" (angl. šešėlinė komanda) buvo tarptautinis internetinis nusikaltėlių forumas, kur karderiai ir programišiai galėjo pirkti ir parduoti vogtą asmeninę informaciją, „nulaužtus" kreditinių kortelių bei padirbtus asmens tapatybės duomenis ir jais keistis.

dinaviancarding.com“ ir daug kitų, o tarp jų viena, pasivadinusi žavinga santrumpa IAACA*, parodijuojančia Amerikos akademinę bendruomenę.

Tačiau nė viena iš jų nebuvo tokia sėkminga, kokia dvejus savo gyvavimo metus buvo „Shadowcrew“. O Raudonoji Brigada buvo vienas iš daugelio Šešėlinės komandos karderių, kuriam pašėlusiai sekėsi. Teisėsauga tik neseniai sužinojo apie šio verslo mastą. Bankai iš esmės dar nieko nenutuokė, o paprasti žmonės į tai nekreipė dėmesio.

Programišiai buvo pažengę toli į priekį, o pinigai valdė visus – alternatyviųjų fondų valdytojus, oligarchus, naftos šeichus, Lotynų Amerikos mobiliųjų telefonų magnatus, naujai įsigalėjusį Pietų Afrikos juodosios ekonomikos elitą, senąjį Pietų Afrikos baltosios ekonomikos elitą, visame pasaulyje populiarių niekniekių gamintojus iš Kinijos, elektroninių technologijų kūrėjus nuo Bangaloro Indijoje iki Silicio slėnio Amerikoje.

Šimtai karderių susikrovė didelius pinigus per „Shadowcrew“, daugelis iš jų, būdami gana naivūs, iššvaistė juos turtingumo simboliams įsigyti. Tais laikais, perkant prekes internetu, nebūdavo tikrinami kompiuterių IP adresai. Nebuvo kreditinių kortelių adresų patvirtinimo sistemos: prekes buvo galima siųsti į bet kurį pasaulio kraštą (išskyrus Rusiją ir kitas buvusias sovietines šalis), nepaisant to, kur kortelė buvo išduota, ir niekas niekada jos kruopščiai netikrindavo.

Šie naujos rūšies nusikaltimai sudygo gerokai toliau nuo savojo ukrainietiškai ir rusiškai kalbančio daigyno. Jie spontaniškai pradėjo plisti visame pasaulyje. Raudonoji Brigada pagalvojo, kad žinomi Azijos nusikaltėliai dabar palaiko ryšius su jaunaisiais kolegomis iš

* IAACA – *International Association for the Advancement of Criminal Activity* – Tarptautinė kriminalinės veiklos pažangos asociacija (angl.), o IACA – *International Anti Corruption Academy* – Tarptautinė kovos su korupcija akademija (angl.).

Masačusetso, bendraujančiais su Rytų europiečiais, kurių kompiuteriai perpildyti šūsnių kreditinių kortelių duomenų. Už kai kurių „Shadowcrew" slapyvardžių slėpėsi tokie kriminalinio pasaulio sambūriai kaip savo bendražygių garbinamas Visa Matantis Fantomas.

Geru dešimtmečiu vyresnis už daugumą Šešėlinės komandos narių, Raudonoji Brigada nematė reikalo įgyti pripažinimo ir pagarbos, stengdamasis užkopti hierarchijos laiptais. Jis nesuprato, kodėl eiliniams nariams tokią pagarbą kelia forumų moderatoriai ir administratoriai. Kad ir kaip jiems sekėsi, Šešėlinės komandos vadovai elgėsi naiviai ir kvailai, beveik vaikėziškai – nieko nuostabaus, nes daugumai jų dar nebuvo nė dvidešimties ar buvo šiek tiek daugiau nei dvidešimt.

Raudonoji Brigada pastebėjo, kad „CarderPlanet" sukūrė ir išvystė tikri nusikaltėliai, o daugelis „Shadowcrew" komandos narių buvo diletantai, kurių beribę puikybę tenkino jų uždirbamos nesuvokiamo dydžio pinigų sumos.

Vėliau Raudonoji Brigada laikėsi atokiai nuo šių veikėjų, o dar mažiau jis norėjo būti susektas teisėsaugos. Visi, išskyrus vos kelis Šešėlinės komandos narius, nė nenujautė, kad Slaptoji tarnyba jau giliai prasiskverbusi į šią interneto svetainę.

2003 m. birželį buvo suimtas jaunas kubiečių kilmės amerikietis, vienas iš seniausių Šešėlinės komandos narių Albertas Gonzalesas. Tarp karderių jis buvo žinomas kaip CumbaJohnny. Bet jie nežinojo, kad po arešto jis tapo informatoriumi. Tai buvo svarbus Slaptosios tarnybos laimėjimas. Gonzalesas valdė vadinamąjį virtualų privatų tinklą, per kurį pagrindiniai svetainės veikėjai bendravo tarpusavyje. Tinkamai eksploatuojamą VPN teisėsaugos institucijoms susekti labai sunku, beveik neįmanoma, nebent jei vyrukas, valdantysis administratorius, bendradarbiauja su policija, kaip buvo Gonzaleso atveju.

2004 m. spalio 26 d. JAV slaptoji tarnyba atliko daugybę reidų visose Jungtinėse Valstijose. Devyniolika asmenų buvo suimti ir apkaltinti veikla „shadowcrew.com“. Dar keli buvo suimti vėliau.

„Shadowcrew“, – teigiama kaltinime dėl kriminalinio sąmokslo, – buvo tarptautinė organizacija, kuriai priklausė maždaug 4 000 narių, dalyvavusių įvairioje kriminalinėje veikloje ar prisidėjusių prie jos.“ Tai buvo didžiausias Slaptosios tarnybos jaunos kibernetinės policijos grupės laimėjimas. Oficialus kaltinimas, pateiktas Naujojo Džersio apygardos teisme, skambėjo dramatiškai. „Administratoriai, – buvo sakoma jame, – kolektyviai kontroliavo organizacijos veiklos kryptis, priimdami kasdienio valdymo sprendimus ir sudarydami ilgalaikius strateginius organizacijos išlikimo planus... Administratoriai turėjo visą prieigą prie serverių, suteikiančių prieglobą „Shadowcrew“ svetainei, ir buvo pagrindiniai asmenys, atsakingi už šių serverių fizinį administravimą, priežiūrą ir saugumą, taip pat ir už svetainės turinį.“

Žiniasklaida azartiškai skubėjo pateikti naujienas apie „Shadowcrew“ žlugimą ir nuėjo taip toli, kad beveik prilygino šį įvykį Korleonės klano iš Sicilijos sutriuškinimui. Nušviečiant šiuos įvykius prisidėjo ir tai, kad viena iš kaltinamųjų buvo moteris Karina Andersson, dar žinoma kaip Kafka, nors Slaptoji tarnyba iš tiesų nesugebėjo atskleisti, kad tikrasis nusikaltėlis buvo jos vaikinas, kuris paprasčiausiai naudojosi jos kompiuteriu ir IP adresu nusikaltimams vykdyti. Žinant, jog 96 procentai programišių yra vyrai, tuo netenka stebėtis.

Šie areštai neabejotinai buvo pateisinami. Tačiau ar „administratoriais“ pasivadinę vyrukai užsidirbdavo pinigų per „Shadowcrew“? Ne. Tiesa, tarp jų buvo keletas vadinamųjų „pinigų kalėjų“ (svarbiausias iš jų buvo Gonzalesas, kuris, nepaisydamas savo artimų ryšių su Slaptąja tarnyba, vėliau sugalvojo dar liūdniau

pagarsėjusį reidą – įsilaužimą į „T. J. Maxx“ parduotuvių tinklo kreditinių kortelių duomenų bazę).

Tačiau policininkai susidūrė su neretai pasitaikančia problema: programišiai nėra tipiški kriminaliniai nusikaltėliai. Tiesa, jų įgūdžiais naudojasi tikri nusikaltėliai, kurie fiziškai nusikalsta gyviems žmonėms. Tačiau programišiai dažnai nekreipia dėmesio į šį savo veiklos aspektą. Jie, Skripto apibūdinimu, yra „vieniši vilkai“, dažnai nesuinteresuoti susikrauti turto, nes jiems labiau rūpi pirmauti savo sugebėjimais tarp bendraamžių. „Turite suprasti, – aiškino JiLsi, prisimindamas savo, kaip karderio, patirtį, – kad visa tai buvo tik žaidimas. Tai tas pats kaip žaisti „Grand Theft Auto“, išskyrus tai, kad čia viską darai iš tikrųjų. Esi priverstas kautis su gyvais policininkais. Tai sukelia daug didesnį jaudulį! Tai susiję su pagarba. Tai susiję su... – JiLsi stabtelėjo, siekdamas didesnio efekto, – tavo autoritetu.“

Tam tikra prasme „Shadowcrew“ internetinių nusikaltėlių suėmimai atkartojo svarbių mafijos organizacijų išardymą realiame pasaulyje. Taip kardingo pasaulyje susidarė tuštuma, kurioje radosi nauja karderių karta, o jos nariai susijungė į dvi naujas kitais metais pasirodžiusias ir dėl viršenybės kovojančias svetaines: „CardersMarket“ ir „DarkMarket“.

IV dalis

14
Ledo žmogus ateina

Santa Klara, Kalifornija, 1998 m. spalis

Maksas Vizija (Max Vision) nustebo, kai Chrisas ir Mike'as, du asmenys iš FTB San Fransisko skyriaus, su kuriais jis palaikė ryšį, pasirodė prie jo paradinių durų Santa Klaroje. Jis nepažino trečio vyriškio, nors vėliau sužinojo, kad tai buvo FTB kompiuterinių nusikaltimų skyriaus viršininkas. Visgi tai nebuvo paprastas vizitas. „Mes ruošiame bylą prieš tave, Maksai, – pasakė jie. – Šį sykį tu rimtai susimovei."

Ištiktas lengvo šoko Vizija parvertė savo kompiuterį. Jis nenorėjo, kad atrodytų, jog jis trukdo vykdyti teisingumą, o ir pats dar nesuprato, kas čia per problema. Jo gyvenimas buvo puikus, netgi nuostabus. Išgyvenęs audringą paauglystę, jis persikėlė iš Ajovos į regioną, kur jokie keistuoliai, jokie netvarkingi ilgi palaidi ar į uodegą surišti plaukai nebuvo laikomi neįprastais ar neelegantiškais. Niekas nesistebėjo ir tuo, kad savo prozišką pavardę Butleris jis pakeitė į Vizija. Jis greitai priprato prie tingaus ir nerūpestingo Vakarų pakrantės gyvenimo būdo, o svarbiausia – buvo karštai įsimylėjęs savo būsimą nuotaką Kimi.

Dar tik įpusėjęs trečią dešimtį, jis jau buvo talentingas kompiuterių apsaugos sistemų specialistas ir vienas iš labiausiai gerbiamų ir didžiai vertinamų konsultantų San Fransisko įlankos regione. Jis taip pat buvo ir pilietiškas, taigi įkūrė svetainę „whitehats.com", skirtą padėti žmonėms ir kompanijoms apsisaugoti nuo piktavališkų internetinių atakų. Misteris Vizija informuodavo apie naujausias „silpnąsias vietas", būdingas populiariai programinei įrangai, ir paaiškindavo, kaip su jomis susitvarkyti.

Silpnosios vietos buvo programišių kasdienė duona. Jos nurodė pagrindinius kelius, leidžiančius patekti į svetimus kompiuterius. Tai buvo gamintojų pražiopsotos skaitmeninės skylės programinės įrangos ir kompiuterinių sistemų apsaugoje. Jei tokia kompanija kaip „Microsoft" ar „Adobe" pastebėdavo, kad koks nors programišius, pasinaudojęs tam tikra silpnąja vieta, prasiskverbė į „Windows" operacinę sistemą ar į tokią plačiai naudojamą taikomąją programą kaip „PDF Reader", ji galėdavo ją „sulopyti", parašydama konkrečią apsaugos sutvirtinimo programą, ją įdiegdama ir taip užblokuodama kelią į naudotojo kompiuterį. Jei naudotojas neatnaujindavo apsaugos sutvirtinimo, kompiuteris likdavo pažeidžiamas, nes virusai galėdavo pasinaudoti ta ypatinga silpnąja vieta.

Toks aukščiausios klasės programišius – saugumo specialistas kaip Vizija dažnai pastebėdavo silpnąsias apsaugos vietas anksčiau nei bet kas kitas, taigi, būdamas draugiškas, jis duodavo kompiuterių naudotojams praktiškų patarimų, kaip apsisaugoti.

Jo geri darbai plačiai paplito. Jis taip pat suteikdavo nemokamas paslaugas San Fransisko FTB skyriui, o FTB agentai su džiaugsmu priimdavo jo pagalbą.

Joks internetinis iššūkis Maksui Vizijai nebuvo per sunkus, jokia silpnoji vieta jam neatrodė per menka ir neprasprūsdavo pro akis. Tačiau, be jokios abejonės, tam, kad galėtų rasti šias silpnąsias vietas, jis turėjo nuolatos tyrinėti kompiuterines sistemas. Jis supra-

to, jog taip susiduria su sudėtinga dilema, turinčia rimtų pasekmių visai kompiuterių pramonei. Norint apsisaugoti nuo nusikaltėlių programišių, žargonu vadinamų „juodkepuriais", kartais būtina, kad „gerasis" programišius, vadinamasis „baltkepuris"*, išsiaiškintų, kaip įsilaužti į sistemą – o tas veiksmas iš esmės yra nelegalus.

Neišvengiama, kad „baltkepuriai" šniukštinėja po dideles viešas kompiuterines sistemas lygiai taip, kaip tai daro „juodkepuriai". Skirtumas tik tas, kad „baltkepuriai" jokių rastų silpnųjų vietų nenaudoja pelnijimosi tikslais. O „juodkepuris" greičiausiai tuo pasinaudos.

Dirbdamas savo mažame namelyje, kuriame gyveno kartu su Kimi, Vizija pastebėjo, kad kas kartą, užtikęs kokią nors tinklo anomaliją ar problemą, jis negali atsispirti troškimui ją ištaisyti. 1998 m. jis pastebėjo, kad tinklai, kuriais naudojasi daugybė vyriausybinių įstaigų, tarp jų ir kai kurie Pentagono padaliniai, gali būti pavojingai pažeidžiami. Tai buvo jų apsaugos sistemų skylė, pro kurią galėjo prasibrauti visokie žalingi kirminai. Įgudę programišiai, dirbantys bet kuriame pasaulio krašte, tiesiogine prasme galėjo sukelti pavojų šimtams tūkstančių vyriausybinių kompiuterių. Vėlgi demonstruodamas patriotizmą ir norėdamas garantuoti savo tautos saugumą, Vizija užpildė šias skyles skaitmeniniu cementu: niekas niekada nebegalės pasinaudoti tuo ypatingu vyriausybės departamentuose esančių sistemų pažeidžiamumu.

* „Juodkepuriai" programišiai (*blackhat hackers*) – tai didžiausi „blogiukai", kurie įsilaužia į saugius kompiuterių tinklus, turėdami piktaviliškų tikslų sunaikinti duomenis ar išvesti tinklą iš rikiuotės. „Baltkepuriai" programišiai (*whitehat hackers*) įsilaužia į kompiuterius nepiktaviliškais tikslais, pavyzdžiui, norėdami patikrinti savo apsaugos sistemas. Internetiniu žargonu „baltkepuriai" dar vadinami „etiškais" programišiais. „Pilkakepuriai" programišiai (*greyhat hackers*) yra „juodkepurių" ir „baltkepurių" derinys. „Pilkakepuris" programišius, pavyzdžiui, gali įsilaužti į kompiuterių sistemą tik tam, kad paskui praneštų administratoriui, jog į jo sistemą buvo įsilaužta. Tada jis gali pasiūlyti už nedidelį mokestį sutvarkyti sistemą.

O tada įvyko lūžis.

Tiek tuo metu, tiek atsigręžus į praeitį, tai atrodo nereikšminga. Tai buvo toks menkas dalykas, toks trumpalaikis veiksmas, kad vargu ar tada apskritai kas nors tai įsidėmėjo: elektronikos pulso beveik neįmanoma apčiuopti. Vienas klavišo spustelėjimas, viena raidė vienoje iš daugybę puslapių užimančių kompiuterinių programų komandų – programišiui iš prigimties tai trunka tik mirksnį. Ogi įvyko tai, kad visuose tuose vyriausybiniuose kompiuteriuose Maksas Vizija paliko atvirą vieną mažytę skylutę, pro kurią tik jis vienas galėjo praįsti. Šiek tiek vėliau įžvalgus kibernetinių nusikaltimų tyrėjas iš Jungtinių Valstijų oro pajėgų pastebėjo šią skylutę ir atsekė jos kūrėją.

Štai kodėl draugai iš FTB pasibeldė į jo duris Santa Klaroje ir pranešė apie jo padangėje besikaupiančius tamsius debesis. „Tu sukėlei visokiausių problemų, Maksai, – sakė jie. – Tai nacionalinio saugumo klausimas. Štai kodėl Oro pajėgos jau čia."

Vizija nusiminė ir pasipiktino. Jis iš anksto buvo nusiuntęs elektroninį laišką ir išdėstęs jiems savo įtarimus apie sistemų pažeidžiamumą ir apie tai, kaip jis planuoja juos patikrinti.

Kiek rimtas buvo šis nusikaltimas? Makso Vizijos veiksmų neskatino nei finansinė, nei jokios kitos rūšies nauda. Priešingai, su šiuo reikalu susijusioms federalinėms įstaigoms jis pats buvo labai naudingas. Be kitų paslaugų, Vizija apsaugojo tokių karinių bazių ir branduolinių tyrimų centrų kaip Brukheiveno ir Livermoro laboratorijos kompiuterių sistemas. O žinant, kad jo padarytas pažeidimas buvo minimalus ir kad jis nieko nepavogė, argi išmintinga buvo vieną iš talentingiausių Amerikos kompiuterininkų kaltinti šiuo nusižengimu?

Oro pajėgų atstovo atradimas ne tik privedė prie Makso Vizijos arešto, apkaltinus jį tyčiniu kirmino praleidimu. Pasekmės buvo dar baisesnės. Ta maža skylutė, „išgręžta" kompiuterinių tinklų įė-

jimo prievaduose, vis didėjo ir didėjo tol, kol virto baisia pragarme: jo laukė Tafto kolonija – į šiaurę nuo Los Andželo esanti federalinė pataisos įstaiga. Vizija sėdo už grotų kaip subrendęs įgudęs programišius, o ne kaip kriminalinis nusikaltėlis. Su profesionaliais nusikaltėliais jis buvo susidūręs tik plepėdamas su savo pažįstamais iš FTB. Žinoma, viskas netrukus pasikeitė, nes Maksas (su visais savo programišiaus įgūdžiais) atsidūrė negriežto režimo kolonijoje, kur daugelis nuteistųjų atlieka bausmę už sukčiavimus ir kitus finansinius nusikaltimus.

Makso reikalai buvo prasti, bet grėsė dar suprastėti. Jam ne tik buvo paskirta bausmė – dveji metai Tafto kolonijoje, bet, negana to, praėjus mėnesiui nuo atvykimo į bausmės vietą, Kimi pranešė jį paliekanti. Žmonos paliktas dėl kito vyro, išsižadėtas buvusių bičiulių iš FTB, Maksas Vizija puolė į giliausią depresiją. Kalėjime jis susipažino su kitu kaliniu, tokiu Jeffrey Normingtonu, ir šis ištiesė jam draugišką ranką, kai apleido visi kiti.

Paleistas iš kolonijos, Vizija negalėjo susirasti nuolatinio darbo, už kurį būtų mokama nors kiek daugiau nei minimalus atlygis. Ieškant darbo, jam buvo pasiūlytos aukštesnės pareigos užsienio apsaugos kompanijose, bet jis buvo paleistas lygtinai, todėl negalėjo gauti paso. Silicio slėnyje niekas nenorėjo įdarbinti žmogaus, kurio CV buvo neištrinamai įrašytas teistumas už kibernetinį nusikaltimą.

Jo skolos didėjo, o neviltis gilėjo. Bet tada vieną dieną vėl pasirodė jo draugužis Normingtonas ir pažadėjo jam padėti rasti kelią iš pragarmės atgal į Kalifornijos saulę. Pakeliui jo laukė gausios gėrybės. Normingtonas pažadėjo jam modernų „Alienware“ nešiojamąjį kompiuterį – kiekvienam programišiui privalomą, bet brangų žaisliuką. Tai tik pradžiai. Jis pasakė, kad ras Vizijai butą ir sumokės už jį. Normingtonas viską suorganizuos.

Mainais už kelias paslaugas.

Nusikaltimas buvo ne vienintelis jam siūlomas pasirinkimas. Buvo ir kitų kelių, kuriuos jis galėjo išmėginti. Vizija galėjo nuvykti pas draugus ir šeimą. Bet jis buvo pavargęs, jautėsi apleistas, o Normingtonas kalbėjo labai įtikinamai. Kitas posūkio taškas. Kitas neteisingas posūkis.

Taip Maksas Vizija, iš esmės geras vyrukas, buvo nusviestas atgal į pragarmę. Jo vietoje pasirodė Ledo Žmogus – iš esmės blogas vyrukas, kurio antrininkas Vizija turėjo FTB kolaboranto įvaizdį.

15
Karderių rinka

Ledo Žmogus iš šalies stebėjo, kaip JAV slaptoji tarnyba pergudravo pagrindinius „Shadowcrew“ protus. Jis laikėsi nuošaliai nuo daugumos iš šios, jo manymu, menkavertės komandos, siekusios internetu apiplėšti naivuolius, bet iš vidaus nesugebėjusios apsisaugoti nuo informatorių, skundikų ir skaldytojų.

Dabar, kai Šešėlinė komanda buvo išvaikyta ir atsirado daugybė pamėgdžiotojų, norinčių ją pakeisti, Ledo Žmogus tvirtai apsisprendė parodyti pasauliui, kaip įveikti įstatymus. O labiausiai jis norėjo įrodyti savo meistriškumą internetinėje erdvėje ir jos vartotojams.

Ledo Žmogus karderių svetaines laikė prekyvietėmis, kuriose vyrauja anarchija, kur uždirbami menki pinigai ir kur svarbiausia yra veikimo laisvė. Jis nuoširdžiai tikėjo, kad tokių specialių „turgaviečių“ kaip jo naujoji svetainė „CardersMarket“, kur žmonės galėtų keistis informacija, sukūrimas pats savaime neturėtų būti laikomas nusikaltimu, nors kai kuriems prekeiviams ir galėtų kilti noras laužyti įstatymus. Jo svetainė, kaip ir kitos panašios svetainės, norėjo įrodyti, kad internetas, priešingai kitoms gyvenimo sritims, neturėtų būti smarkiai varžomas vyriausybės, todėl svetainės pradiniame puslapyje jis gana tiesiai kreipėsi į policiją ir interneto administratorius:

PRANEŠIMAS TEISĖSAUGAI, PRIEGLOBAI ir
INTERNETO PASLAUGŲ TEIKĖJAMS:

„CardersMarket“ yra **legalus** forumas, vieta, kur jo nariai gali aptarinėti savo pasirinktas temas. Jokios nelegalaus turinio diskusijos NĖRA leidžiamos, o bet kokius nelegalaus

> turinio pranešimus personalas nedelsdamas panaikina. Diskutuoti nėra nusikaltimas. Forumo funkcionavimas nėra nusikaltimas. Čia nerasite kreditinių kortelių numerių, banko sąskaitų, nelegalios programinės įrangos ar bet ko, kas būtų nelegalu Jungtinėse Valstijose ar tarptautiniu mastu. Bet kokia tarp mūsų narių vykstanti įtartina veikla **nėra mūsų reikalas**, o jei taip atsitinka, tai vyksta **už mūsų forumo ribų**. Mes netoleruojame jokios nelegalios veiklos ir jokiais būdais joje nedalyvaujame.

Kuo labiau jis įsitraukė į kardingo pasaulį, tuo labiau susipainiojo savo moralinėse nuostatose. Kaip Ledo Žmogus, jis niekada nepirko ir nepardavinėjo kreditinių kortelių. Bet jomis prekiavo kitas Vizijos sukurtas internetinis veikėjas. Programišiai plačiai naudojasi asmenybės suskaidymo galimybe. Kartais Vizijai ir pačiam imdavo atrodyti, kad jo virtualūs antrininkai savo mintimis ir poelgiais yra anonimiški, ir todėl jie yra individualios esybės.

Ledo Žmogus, norėdamas pasirodyti neginčytinu kardingo žinovu, siekė įveikti tiek savo varžovus nusikaltėlius, tiek policiją. Tam reikėjo panaudoti dvigubą strategiją. Visų pirma jis privalėjo nustatyti ir demaskuoti visus skundikus (konfidencialius informatorius, arba CIs) ir policininkus, kurie persekiojo karderių forumus ir varžėsi dėl pranešimų apie nusikaltimus.

Daug anksčiau, nei JAV slaptoji tarnyba sėkmingai išardė Šešėlinę komandą, Ledo Žmogus išsiaiškino, kad keletas pagrindinių jos narių buvo arba Amerikos ar Kanados teisėsaugos informatoriai, arba prityrę policijos pareigūnai. Tokie veikėjai kaip Ledo Žmogus, užsiimantys apgaulėmis, suvokė, kad jie turi būti įgudę pastebėti tokius pat kitų sugebėjimus. Tiek patyrę internetiniai vagys, tiek kibernetinė policija gerai žinojo, kad niekas taip neskatina maskavimosi ir veidmainiavimo kaip internetas. Todėl, Ledo Žmogaus nuomone, atskleisti skundikus buvo esminė jo darbo dalis.

Kai Ledo Žmogus atskleisdavo informatorius, skambiomis sarkastiškomis frazėmis pranešdavo apie juos forumuose. Kai kurie forumų nariai nusprendė, kad jis per daug reiškiasi. O gal pagrindinis „CardersMarket" protas ir pats yra informatorius? Taip iš tiesų atrodė, kai jis ryžtingai ėmėsi savo meistriško plano sutriuškinti varžovus ir gausiai atakavo konkuruojančius karderių forumus, siekdamas juos sunaikinti, o didžiules jų narių duomenų bazes perimti į savo Karderių rinką. Vizija neslėpė savo ketinimų: su nepaprastu įžūlumu jis pareiškė netikįs, kad kitos kriminalinės svetainės, tokios kaip „scandinaviacarding.com" arba „TalkCash", turi teisę egzistuoti.

Norėdamas pabrėžti savo pranašumą, jis pirmiausia sukūrė apgaulingą skaitmeninį taką, kad atrodytų, jog „CardersMarket" serveris yra Irane, taigi sunkiai pasiekiamas tiek teisėsaugai, tiek kitiems internetiniams sukčiams – karderiams. Iš tiesų serveris buvo Kalifornijoje, tačiau Ledo Žmogus sugebėjo taip puikiai gudrauti, kad iš tiesų visus įtikino, jog serveris yra Irane. Savaime suprantama, tai dar labiau įsuko gandų malūną: gal Ledo Žmogus yra Irano žvalgybos agentas, įpareigotas pasėti abejones JAV teisėsaugoje ir surinkti pinigų savo slaptoms operacijoms?

Kad ir kas jis buvo, visi suprato, jog vyras neabejingas šiam verslui. Jis paeiliui sėkmingai įsilaužė į konkurentų kardingo svetaines, „išpumpavo" jų duomenų bazes su visų narių adresais ir slaptažodžiais ir visais korespondencijos įrašais. Paskui visą tą informaciją suvedė į „CardersMarket", o tada panaikino visus įrašus originaliose svetainėse.

Ledo Žmogaus atakos buvo negailestingos – net rusai neišvengė jo keršto. Su beatodairiška narsa jis įsilaužė į „mazafaka.ru", visų Rusijos programišių pamėgtą svetainę, pakeitusią jų mylimą „CarderPlanet". Tačiau nors vyro ego kartais neracionaliai paveikdavo jo sprendimus, Ledo Žmogus puikiai suprato, kad sugriauti rusiškas svetaines taip, kaip sugriovė angliškas, yra labai neišmintinga. Rusai turėjo kelis puikiausius programišius pasaulyje, o

Ledo Žmogus nenorėjo jų išprovokuoti. Dar daugiau, išardžius „Shadowcrew" rusai skubiai išsinešdino iš kardingo draugijos. Tai yra daugiau ar mažiau masiškai jie paliko anglakalbių forumus. Visi tie gausūs nusikaltėlių, informatorių, šnipų ir policijos pareigūnų tarpusavio veiksmai erzino ir darėsi nepakeliami: jie trukdė verslui. Laikydamiesi atokiau nuo šalių, kuriose turi galios amerikiečių teisėsauga, rusai smarkiai sumažino savo veiksmų riziką.

Taip rusų programišiai įkūrė ne vieną forumą, kurie buvo grynai ar daugiausia rusakalbiai, tarp jų ir „mazafaka.ru". JAV teisėsauga įsitikino, kad į juos daug sunkiau prasiskverbti, o bendradarbiauti su Rusijos policija ar dar įtakingesniu KGB pasirodė itin sunkus uždavinys. Pirmoji Rusijos ir Ukrainos kriminalinių programišių gynybinė linija visuomet buvo ir yra nuolat besikeičiantis vietinis žargonas. Nors kai kurie Vakarų policijos pareigūnai sugeba bendrauti rusiškai, jiems yra daug sunkiau neatsilikti nuo dinamiškų populiariajai kultūrai būdingų kalbos pokyčių, mat labai retas žmogus Vašingtone ar Londone gali su jais suspėti.

Tuo metu, kai rusiškos svetainės sėkmingai vystėsi, iki 2006 m. vasaros Ledo Žmogus jau buvo sunaikinęs beveik visus anglakalbius priešininkus. Ir vos tik pastebėjęs, kad kuris nors iš jų bando prisikelti, jis pradėdavo triuškinančią DDoS ataką.

DDoS atakos – plačiausiai paplitęs internetinės erdvės ginklas. Šioms atakoms vykdyti naudojami kenkėjiškomis programomis užkrėsti kompiuterių tinklai (angl. *botnets*), kuriais persiunčiamas elektroninių žinučių brukalas. Šie tinklai – tai tarsi klasikinio šeštojo dešimtmečio Holivudo filmo „Kūnų grobikų įsiveržimas" (*Invasion of the Body Snatchers*) internetiniai atitikmenys. Per ataką virusas „užgrobia" kompiuterį, o tada šis patenka vadinamojo komandų ir kontrolės (KK) serverio įtakon. Tokiu būdu virusas gali užkrėsti tūkstančius kompiuterių, kurie nuo tada vadinami zombiais ir tampa tranais, vykdančiais galingo KK serverio įsakymus. Dau-

geliu atvejų jie ir toliau funkcionuoja kaip normalūs kompiuteriai. Paprastas vartotojas nė neįtars, kad jo kompiuteris tapo didžiulės skaitmeninę mirtį nešančios armijos kareiviu. Jei zombis yra ypač aktyvus, nekalta auka gali pastebėti, kad jos kompiuteris dirba šiek tiek lėčiau, o paprastai taip yra dėl to, kad jis „persidirbo", nepastebimai padėdamas paskirstyti milijardus įbruktų elektroninių žinučių, pavyzdžiui, reklamuojančių penio pailginimo būdus ar „Vicodin" vaistus arba persiunčiančių naujas viruso kopijas, galinčias užkrėsti dar daugiau kompiuterių.

Dažnai užkrėstiems kompiuterių tinklams duodamas nurodymas pradėti DDoS atakas, o visiems zombiams liepiama vienu metu patekti į tam tikrą svetainę. Jei svetainė ar serveris pakliūva į DDoS ataką, jie paprasčiausiai užstringa, negalėdami susidoroti su tokiu dideliu perduodamos informacijos kiekiu. Tinklalapis „sustingsta". Jei ataka pakankamai galinga, užstringa visa sistema.

Dėl savo nenuilstamų DDoS atakų ir arogancijos Ledo Žmogus užsitarnavo kriminalinių programišių bendruomenės neapykantą. Ši taktika taip pat sukėlė įtarimų, kad jis dirba Federaliniam tyrimų biurui, nes jo aukomis tapo labai daug programišių ir nusikaltėlių.

Visgi niekas negalėjo varžytis su jo mastu ir apyvarta, nes „CardersMarket" dabar turėjo kelis tūkstančius aktyvių narių, perkančių ir parduodančių kreditines korteles, bankų sąskaitas, virusus, asmens tapatybės duomenis ir visa kita. 2006 m. rugpjūtį jis jautėsi esąs internetinio pasaulio valdovas.

Tik vienas dalykas jam nedavė ramybės. Vienos kriminalinės svetainės buvo neįmanoma numarinti. Kas kartą, kai ją atakuodavo, sunaikindavo duomenų bazę ir ištrindavo visus jos failus ar kai savo zombių armijoms duodavo komandą panaikinti ją internete, ši vėl atsirasdavo kaip tas juokingas žaisliukas stovukas, kuris nuverstas vėl visada atsistoja.

Taip prasidėjo kova su Tamsiąja rinka.

16
Tamsioji rinka

Internetas, 2005–2008 metai

Automobiliui su itin galingu varikliu leidžiantis vakariniu Alpių pakraščiu, virš gaiva alsuojančios Vidužemio jūros suspindo saulė, stiprindama nuostabaus ateinančio savaitgalio pažadą. Grupė ne ką vyresnių nei dvidešimties metų jaunuolių iš Skandinavijos, vadovaujamų Švedijos karderių karaliaus Reckos, įsuko iš A8 į Didžiojo Skardžio greitkelį, o tada kalnais žemyn nuvinguriavo į Monaką.

Ši kunigaikštystė, viena iš mažiausių ir tankiausiai apgyventų pasaulio šalių, didžiąją praeito amžiaus dalį maudėsi savo kerinčiame spindesyje. 1956 m. ji tapo pokarinio pasaulio garsenybių auksiniu etalonu, kai viena iš geidžiamiausių Holivudo princesių Grace Kelly įsiliejo į karališkąją šeimą, ištekėjusi už Monegaskų (Monako) sosto įpėdinio princo Rainierio.

Dabar, praėjus lygiai penkiasdešimčiai metų po garsiausių Monako šimtmečio vestuvių, grupė Tamsiosios rinkos narių, prisikimšusių kišenes neįprasto grobio – vogtų plastikinių kreditinių kortelių, trumpam išsiruošė į šią dekadanso šventovę. Kai jie kirto Prancūzijos ir Monako sieną, akiratyje netrukus pasirodė pirmieji kazino. Šie grynųjų pinigų fabrikai nuo devyniolikto amžiaus septintojo dešimtmečio yra kunigaikštystės biudžeto garantas. Vietiniai juos vadina „Monako pinigine“ ir vien dėl jų Monako gyventojai nemoka mokesčių. O kam jiems to reikia? Pavyzdžiui, vienvietis kambarys Monte Karlo viešbutyje „Bay Hotel“ kainuoja 800 dole-

rių už naktį, ir jei svečiai gali sau tai leisti, jie, be abejo, gali švaistyti pinigus lošdami kazino. O tai atspindi visuotinį perteklių.

Taigi vietos gyventojai ramiai maudosi didžiuliuose piniguose, o didžiausi turtuoliai švaisto juos kortuodami ir lošdami rulete. Čia gyvenantys atvykėliai iš kitur dažnai jaučiasi galį lengvai apsieiti be šių pinigų, nes kitomis aplinkybėmis išleistų juos mokesčiams valstybės iždui tų šalių, kuriose jie praleido daugiausia laiko arba kuriose ilgiausiai gyvavo jų verslas. Kadangi Monakas yra rojus žmonėms, vengiantiems mokėti mokesčius, o remiantis pagarbos nusipelniusia Ekonominio bendradarbiavimo ir plėtros organizacija – taip pat ir norintiems išplauti pinigus, šios uolomis nusėtos laisvos nuo mokesčių vietovės valdžios organai nepratę klausinėti savo mažos šalies lankytojų apie jų pinigų kilmę.

Taigi tai puiki vieta grupei Tamsiosios rinkos narių, apsirūpinusių dvylika „American Express Centurion" kortelių. Šios kortelės, neoficialiai vadinamos juodosiomis „Amex" kortelėmis, yra tarsi kokios plastikinių kreditinių kortelių amžiaus olimpinės dievybės, nes pagal specialų kvietimą suteikiamos tik didžiausiems piniguočiams iš Vakarų šalių, Japonijos, Honkongo ir Artimųjų Rytų. Amerikoje „Centurion" kortelės turėtojas turi mokėti 5 000 dolerių stojamąjį mokestį, o paskui kasmetinį 2 500 dolerių mokestį. Užtat mainais jis gauna nemokamus lėktuvo bilietus, atsidavusio durininko paslaugas, asmeninį padėjėją apsipirkinėjant ir narystę elitiniuose klubuose, apdairiai išmėtytuose po visą pasaulį, apie kuriuos mes, eiliniai Juodadarbių planetos gyventojai, neturime nė mažiausio supratimo.

O kaip su grynaisiais? Pateikite savo „Centurion" kortelę ir galėsite maudytis euruose, sterlinguose, šveicariškuose frankuose ar jenose, kuriuos banko kasininkas įteiks jums su vos pastebimu šypsniu, tausojamu jūsų vertės ir padėties žmonėms. Vienos „Centurion" kortelės beveik užtektų, norint sumokėti išpirką už Somalio piratų į nelaisvę paimtus įkaitus.

Nieko nestebina grupė pinigų pertekusių jaunuolių, netikėtai atvykusių į Monte Karlą su savo „Centurion" kortelėmis ir norinčių išlaidauti, išlaidauti ir dar kartą išlaidauti – šioje aplinkoje įprasta matyti išlepintus vaikėzus. Jie buvo ryžtingai nusiteikę iki galo išnaudoti savo dvylika magiškų žetonų. Pirmiausia – prabangus viešbutis, paskui kokteiliai ir ištaigingi valgiai, o tada kazino puolimas. „Tai buvo beprotiškas vakarėlis, – svajingai prisimena vienas iš jų, – 2006-ieji buvo tie metai, kai „DarkMarket" pradėjo skrajoti padebesiais." Kai jaunieji karderiai po poros dienų išvyko, iš savo juodųjų „Amex" kortelių jie buvo paėmę 400 000 dolerių. Jie netgi pripažįsta buvę pritrenkti, kaip lengva buvo tai padaryti. „Niekas nė nemirktelėjo. Niekas nė sykio mumis nesuabejojo. Jautėme, kad tokius dalykus žmonės daro nuolatos."

Skandinavai buvo ne vieninteliai, kuriems pasisekė užsidirbti daug pinigų. Žinomas Ukrainos karderis Maksikas susišlavė šimtus tūkstančių dolerių, perparduodamas vogtas ir klonuotas kreditines korteles ir kreditinių kortelių numerius kartu su PIN kodais ir trimis skaičiais, esančiais kitoje kortelės pusėje. Veikėjas iš Turkijos, pasivadinęs Cha0, sukūrė tikrą kriminalinės veiklos įmonę: paversdavo klonuotų kreditinių kortelių turinį grynaisiais pinigais ir parduodavo kreditinių kortelių nuskaitymo prietaisus kitiems vagims visame pasaulyje, kad jie patys galėtų vogti kortelių duomenis.

„Darkmarket.com" buvo įkurta 2005 m. gegužę, bet kelis pirmuosius jos egzistavimo mėnesius tai buvo nelabai gyvybinga afera. Tačiau tų pačių metų rudenį svetainė pritraukė keletą reikšmingų figūrų iš kitų kardingo forumų. Energingiausiai reiškėsi programišius iš Šri Lankos, pasivadinęs JiLsi, jau įkūręs svetainę „The Vouched" ir įgijęs moderatoriaus statusą mažoje, bet įtakingoje forumo „mazafaka" anglakalbių sekcijoje.

Visai netrukus JiLsi buvo paskirtas „DarkMarket" pasauliniu moderatoriumi, kuris yra tik viena pakopa žemiau už svarbiausią

statusą turintį asmenį – administratorių. Jis pats apsiėmė patobulinti „DarkMarket" profilį. JiLsi siekė to paties, ko Ledo Žmogus siekė „CardersMarket" svetainei: jis norėjo, kad anglakalbių pasaulyje ji būtų pripažinta aukščiausio lygio kriminaline svetaine. Nenuilstamai dirbdamas šiauriniame Londone įsikūrusioje „Java Bean" interneto kavinėje, iki 2006 m. gegužės jis sugebėjo pritraukti šimtus naujų narių. Dauguma iš jų buvo anglakalbiai, nors į ją užklysdavo ir nemažai rusų.

Kai tik „DarkMarket" svetainė išpopuliarėjo tarp viso pasaulio karderių, jos įkūrėjai nusprendė uždaryti Tamsiąją rinką, nes bijojo, kad į ją gali prasiskverbti saugumo tarnybos. Vienas iš jų netgi nerimavo, kad ji tampa per daug populiari. JiLsi ir jo draugužiai, norėdami dar labiau padidinti savo augantį autoritetą, paprasčiausiai perregistravo svetainę kaip „darkmarket.ws" (su Vakarų Samoa domenu).

Dabar jie iš tiesų galėjo kibti į darbą. Be JiLsi, Tamsioji rinka galėjo pasigirti įžymaus Rusijos programišiaus, veterano iš „CarderPlanet" slapyvardžiu Štirlicas, parama. Jis veikė kaip tarpininkas tarp rusų kardingo svetainių ir Tamsiosios rinkos.

Buvo ir daugybė kitų. Į Tamsiąją rinką žvalgėsi Matrica. Jo, kaip grafinio dizaino specialisto, autoritetas pradėjo augti nuo tada, kai jis tapo Tarptautinės kriminalinės veiklos pažangos asociacijos nariu. Tai, ką pamatė, jam nepadarė įspūdžio – diskusijų forumas buvo skurdus, o jo apsauga menka. Administratoriui JiLsi jis nusiuntė tiesmukišką žinutę, pažymėdamas, kad dėl netinkamos programinės įrangos tokie priešai kaip Ledo Žmogus bet kada gali įsiveržti į svetainę. Matrica pasiūlė įdiegti geresnę sistemą. JiLsi tam pritarė, ir taip Matrica pradėjo kilti hierarchijos laiptais.

Buvo ir daugiau norinčiųjų jiems padėti. JiLsi ilgai negalvodamas pasiūlė užimti forumo moderatoriaus vietą kažkokiam Meistrui Splyntrui (Master Splyntr). Po šiuo slapyvardžiu slėpėsi žinomas lenkų elektroninio brukalo siuntinėtojas Pavelas Kaminskis.

Mąstant paauglių sąvokomis, jo slapyvardį buvo galima susieti su žiurke iš populiaraus animacinio filmuko vaikams, išmintinguoju sensei*, Meistru Splinteriu, kuris paauglius mutantus vėžliukus nindzes mokė kautis. Pagerbiant šį herojų ir jo gebėjimus, Meistras Splyntras internetinių sukčių bendruomenėje buvo taip pat vadinamas sensei.

Tikrąją Meistro Splyntro asmenybę atskleidė slapta Britanijos kovos su internetiniais sukčiais organizacija „spamhaus.org". Verslininkai, technokratai, buvę šnipai ir dievai žino kokie dar veikėjai, sudarantys šią komandą, surengė veiksmingą kampaniją ir įtraukė į juoduosius sąrašus pačius azartiškiausius elektroninio brukalo siuntinėtojus, sukčiautojus su kreditinėmis kortelėmis ir vaikų pornografijos paltintojus. Kampanijos tikslas – apvalyti skaitmeninį pasaulį nuo nenaudėlių interneto paslaugų teikėjų, kurie nepastebi nusikalstamos savo naudotojų veiklos. Kaminskis, kaip pranešė „Spamhaus" savo svetainėje, buvo vienas iš penkių svarbiausių elektroninio brukalo siuntinėtojų, atsakingų už milžiniškus kiekius nereikalingų reklamų apie penio didinimą, „Vicodin" vaistus ir kitą šlamštą.

„Spamhaus" susidomėjimas Meistru Splyntru reiškė, kad jis yra žymus žmogus, taigi tada, kai nuo brukalo siuntinėjimo elektroniniu paštu jis perėjo prie sukčiavimo su kreditinėmis kortelėmis, penkios policijos pajėgų institucijos iš viso pasaulio ryžtingai ėmėsi tyrinėti jo veiklą. Kaminskis taip pat buvo susijęs su kenkėjiškų programų, virusų ir trojanų didmeniniu paskirstymu. Jis buvo pripažintas nedorėlis, taigi JiLsi buvo gan smarkiai sujaudintas, kad jam pavyko įvilioti tokią didelę žuvį į Tamsiosios rinkos vandenis. JiLsi buvo dėmesingas tiek Splyntrui, tiek Matricai. Jie visi sudarė gana

* *Sensei* yra japoniškas žodis, kuris iš esmės reiškia „asmuo, gimęs anksčiau už kitus". Plačiąja prasme jis vartojamas kaip „meistras" arba „mokytojas".

neblogą komandą, o prie jų prisidėjus Turkijos nusikaltėlių vadeivai Cha0, „DarkMarket“ įgijo neabejotinos sėkmės aurą.

Atidžiau įsižiūrėjus, „DarkMarket“ nebuvo tokia jau nepaprasta. Ji funkcionavo lygiai taip pat kaip ir kiti interneto forumai, kurie, tarkim, aptarinėja vaikų auklėjimą ar bičių auginimo ypatumus. Prie jos buvo sunkiau prieiti, nes jos nariai buvo priimami vetavimo principu, bet tai nesudarė didelės kliūties tiems, kurie buvo susipažinę su kardingu ir pasiryžę prie jos prisijungti. Saugumo sumetimais tikrasis verslas – pirkimas ir pardavimas – vargu ar kada nors buvo vykdomas per forumą. Tai daugiau buvo pardavėjų ir pirkėjų susitikimo vieta; būtent čia galėjo rasti rinką gaminantieji nelegalius kreditinių kortelių nuskaitymo prietaisus („skimerius“); o turintieji kreditinių kortelių duomenų bazes galėjo suformuoti komandą, kuri atliktų pinigų išgryninimo darbą (tą pavojingą darbą, kai, einant nuo vieno bankomato prie kito, reikia paimti grynuosius iš sąskaitų). Tačiau bet kokių sandėrių detalės beveik visuomet būdavo aptariamos privačiuose šifruotuose pokalbiuose, vykstančiuose per apsikeitimo žinutėmis programos „Icq“ tinklus. Kai sandėris būdavo sudarytas, jo partneriai grįždavo atgal į svetainę užsakyti sąlyginių įsipareigojimų paslaugos, taigi prašydavo administratoriaus užtikrinti, kad žaidimas vyktų sąžiningai.

Forumas kas kartą pritraukdavo vis daugiau narių, taigi verslas klestėjo. Pagrindiniai asmenys buvo tiltas tarp rusų nusikaltėlių ir karderių iš Vakarų, tačiau tuo pat metu JiLsi pastebėjo, jog narių geografija plečiasi. Turkija pradėjo reikštis kaip svarbi internetinių nusikaltimų šalis. Labai greitai didėjo Ispanijos ir Vokietijos bendruomenės, netgi Prancūzijoje, kurios karderiai, kaip ir dauguma prancūzų, net ir internete geriau jautėsi prancūziškai kalbančiųjų aplinkoje, tobulino savo anglų kalbą, kad galėtų stoti į grumtynes.

Tamsioji rinka buvo pakeliui į savo Aukso amžių.

17
Biuras

Renu Subramaniamui biurą atstojo jo terminalas „Java Bean" interneto kavinėje. Per pastaruosius aštuoniolika mėnesių Renu dažniausiai naudojosi internetu džerškėjimo ir riksmų fone, nes nedidukė „Java Bean" kavinukė slėpėsi Vemblio stadiono šešėlyje, o jame tuo metu buvo atliekama monumentali rekonstrukcija, kurią 2006 m. viduryje buvo vėluojama užbaigti ir kurios biudžetas jau buvo viršytas.

Daugeliu atžvilgių kavinė nesiskyrė nuo tūkstančių kitų viso pasaulio kavinių. Įsikūrusi nepatrauklioje aplinkoje tarp kėglinės ir nušiurusios nuomojamos buhalterio kontoros, ji buvo priglaudusi keletą pasitikėjimo nekeliančių kompiuterių su aptriušusiais griozdiškais monitoriais ir nučiupinėtomis klaviatūromis, ant kurių buvo išraižyti pavadinimai, žymintys, jog tai pigūs Rytų Azijos gaminiai. Vienas Dievas žino, kokia veikla vyko už išklibusių medinių pertvarų, skiriančių purvinus valdymo pultus.

Palinkę prie ekranų, paaugliai valandų valandas žaidė internetinius žaidimus, dažnai sugebėdami neįtikėtinai rimtai susikaupti; jauni žygeiviai, teišgalintys keliauti su kuprinėmis ant pečių, kūrė nuostabius elektroninius laiškus, kupinus įspūdžių apie naujai atrastus kraštus; smalsūs paaugliai ir nusivylę vidutinio amžiaus vyrai naršė paslaptingas pornografines svetaines; jauni idealistai planavo politinius protestus, įsivaizduodami, jog pasisakydami šiuose anonimiškuose susirinkimuose jie išsisuks nuo Didžiojo Brolio; narkotikų prekeiviai tarėsi dėl narkotikų permetimo punktų ir pinigų plovi-

mo; o internetiniai nusikaltėliai prisijungdavo, norėdami išsiaiškinti naujausio savo grobio vertę.

Be to, kad buvo įsikūrusi nebaigto įrengti Vemblio stadiono šešėlyje, „Java Bean“ turėjo dar vieną ypatumą. Paprastai interneto kavinių kompiuteriai būna labai menkai apsaugoti nuo išorinių atakų. Virusai, trojanai ir kitos skaitmeninės bakterijos telkiasi šiose vietose dar labiau nei jų organinės kilmės ekvivalentai nerūpestingai valomose ligoninėse.

Tačiau Renu į savo saugumą žiūrėjo rimtai, taigi jis įkalbėjo „Java Bean“ šeimininką kavinės kompiuterinėse sistemose įdiegti specialią programą pavadinimu „Deep Freeze“*. Ji atkūrė ankstesnę standžiojo disko konfigūraciją, užtikrinančią, kad kompiuteriai „nebeįsileis“ jokių kasdien atsiunčiamų kenkėjiškų programų, nereikalingas programas pavers neveiksmingomis ir taip sustiprins Renu apsaugą.

Jei „Java Bean“ interneto kavinę laikysime Renu biuru, tada mažytę duomenų laikmeną – atmintuką (angl. *memory stick*) galime pavadinti jo dokumentų spinta, kurioje buvo saugomos „DarkMarket“ paslaptys. Paprastai savo nešiojamąjį standųjį diską Renu laikydavo tikrąja šių žodžių prasme prie širdies. Atvykęs į biurą, jis įkišdavo atmintuką į vieną iš kompiuterinių terminalų ir pradėdavo dirbti Tamsiojoje rinkoje.

Prisijungęs prie svetainės, Renu užsidėdavo pirato kaukę ir tapdavo JiLsi, vienu iš aštuonių administratorių, valdžiusių Tamsiąją rinką trejus jos egzistavimo metus. Administratorių komanda, kurią visada sudarė ne daugiau nei keturi nariai, buvo viena iš įtakingiausių pasaulinėje kardingo scenoje. Šis aukščiausias postas davė nedaug papildomų pajamų, bet tai buvo privilegijuotos pareigos, užtikrinančios didelę pagarbą tarp programišių ir įsilaužėlių. Jie taip

* Gilus įšalas. (Angl.)

pat mėgavosi prieiga prie milžiniškų informacijos talpyklų ir savo rankose turėjo raktus nuo virtualaus gyvenimo ir mirties vartų – galią pašalinti narius už tikrus ar tariamus nusižengimus.

Šios aukštos administratoriaus pareigos turėjo du pagrindinius trūkumus. Visų pirma tai buvo labai sunkus darbas, kai visą laiką po penkiolika septyniolika valandų per parą esi „prikaltas" prie klaviatūros. Šie žmonės neatostogaudavo – bet kurią dieną jie turėjo būti pasiekiami telefonu. Pavyzdžiui, Meistras Splyntras su savimi visada nešiojosi mobilųjį telefoną, jei būtų reikalingas kuriam nors iš Tamsiosios rinkos bičiulių. Jis atsiliepdavo į kiekvieną skambutį. JiLsi skųsdavosi, kad turi prisijungti devintą ryto ir sėdėti iki dešimtos vakaro. Buvo daug nuobodaus darbo: reikėjo kontroliuoti, ar nariai tvirtai laikosi forumo taisyklių, ir tikrinti, ar savo pranešimus jie skelbia tinkamose forumo sekcijose. Daug laiko užimdavo paprasčiausia biurokratija, dažniausiai nereikšminga ir bukinanti protą.

Antra, administratorių komandai visada buvo prieinami vidiniai kriminalinių svetainių klodai. Skaitmeninis pėdsakas, kurį ji paliko internete, buvo daug ryškesnis nei eilinių narių, todėl administratoriai pirmiausia tapo kibernetinės policijos taikiniu.

Tai buvo paradoksalu, nes paprastai būtent eiliniai nariai Tamsiojoje rinkoje uždirbdavo daugiausia pinigų: administratoriai dažnai prisiimdavo didžiausią riziką už mažiausią finansinį atlygį. Per trejus metus JiLsi ir Matrica užsidirbo menkus pinigus, o Meistras Splyntras buvo atsakingas tik už serverių priežiūrą, taigi didžiausią dėmesį galėjo skirti kitiems internetinių sukčių imperijos reikalams.

Beveik nuo pat pradžių tarp jų buvo dar vienas įdomus veikėjas, pasivadinęs Štirlicu (Shtirlitz). Slapyvardis susijęs su iš beletristikos žinomu Maksu Otu fon Štirlicu. Juliano Semionovo romanuose Štirlicas per Antrąjį pasaulinį karą buvo aukštesnysis nacių kari-

ninkas, Maskvos slaptasis agentas. Apibūdinamas kaip sovietinis Džeimsas Bondas, Štirlicas rusų sąmonėje praeito amžiaus aštuntajame dešimtmetyje įsitvirtino per seriją populiarių filmų, paremtų Semionovo knygomis. Ramus, tačiau nepaprastai išvaizdus Štirlicas pokomunistinėje Rusijoje iki šių dienų išliko galingu patriotiniu simboliu dėl begalinės drąsos, protinių gabumų ir nepalaužiamo atsidavimo tėvynei.

Taigi mes žinome Štirlicą – sovietinį šnipą, bet kas toks buvo karderis Štirlicas (kas transliteravo jo vardą iš rusų į anglų kalbą, pridėdamas raidę h*)? O gal jis taip pat buvo ir KGB agentas? Arba dvigubas agentas, dirbantis Federaliniam tyrimų biurui ar Slaptajai tarnybai? Ar tai buvo kardingo meistras? Vienas jį pažinojęs „CarderPlanet" narys apibūdino jį kaip „apie trisdešimties metų, panašų į ariją" vaikiną. Jis nuolatos pirkdavo padirbtus pasus ir vienu metu gyveno Čekijos Respublikos sostinėje Prahoje. Karderių planetoje jis buvo laikomas „geru ir patikimu vyruku", bet vėliau kiti karderiai pradėjo įtarti, kad galbūt jis, sekdamas savo literatūrinio herojaus pavyzdžiu, palaipsniui virto vienu iš labiausiai prityrusių Amerikos teisėsaugos pareigūnų.

Kad ir kokie buvo Štirlico, kaip vieno iš vyresniųjų „DarkMarket" narių, tikrieji tikslai, jis buvo tylus, bet visur esantis, nors svetainės veikloje dalyvavo palyginti mažai. Panašiai kaip ir vėliau forumo administracijos nariu tapęs Lordas Cyrikas (Lord Cyric), kuris visai nedalyvavo pirkimo ir pardavimo sandėriuose. Abu jie labai rūpinosi svetainės išlikimu, tuo pat metu mėgaudamiesi savo legendiniu statusu tarp bendrijos narių.

Vis dėlto kiekvienas iš jų turėjo ir savų paslapčių, ir kai kurios iš jų buvo visai ne tokios, kaip būtų galima įtarti.

* Rusų šnipas Štirlicas angliškai rašomas *Stirlitz*, o čia aprašytas karderis – *Shtirlitz*.

Ironiška, kad tas, kuris rimčiausiai rūpinosi savo asmeniniu saugumu, tam tikra prasme buvo labiausiai perregimas. Tas asmuo buvo Cha0. Turkų nusikaltėlis palyginti vėlai įsitraukė į karderių forumus. Skirtingai nuo kitų, jis nebuvo „Shadowcrew" ar IAACA veteranas, bet atsirado nežinia iš kur 2006 m. pradžioje kaip svetainės „crimeenforcers.com" savininkas. Tai buvo elegantiško dizaino svetainė, kuri sėkmės trokštantiems internetiniams nusikaltėliams siūlė visų rūšių atsarginių kopijų paslaugas. Svetainė buvo ypač įsidėmėtina dėl savo animacinių pamokų, kuriose karikatūrinis Cha0 herojus supažindino žiūrovus su subtiliais kardingo klausimais.

Cha0 naudojosi Tamsiąja rinka savo svetainei „crimeenforcers.com" reklamuoti (mokama reklama forumams buvo svarbus įplaukų šaltinis), o kadangi jis visur dalyvavo ir nenuilstamai sudarinėjo verslo sandėrius, tai greitai ėmė daryti realią įtaką. Jis įstojo į Tamsiąją rinką 2006 m. vasarį ir po septynių mėnesių buvo paskirtas vienu iš jos vadovų.

Kitaip nei jo kolegos, jis priklausė retai rūšiai. Tai buvo programišius fanatikas, turintis nuostabių nusikaltėliškų sugebėjimų. Jo motyvacija sutikti eiti aukštas pareigas buvo labai paprasta: jis galėjo jomis pasinaudoti plėtodamas savo verslą. Jis pardavinėjo reikmenis, reikalingus ekonominiams nusikaltimams vykdyti, pavyzdžiui, nelegalius skaitytuvus – įrengimus, skirtus aukos kreditinių kortelių duomenims nuskaityti, saugoti ir perduoti.

Tačiau lygiai taip, kaip atsitiko ir kitoms vadovaujančioms „DarkMarket" figūroms, galiausiai pasirodė, kad Cha0 istorija yra žymiai sudėtingesnė ir ganėtinai būdinga Stambulo gyventojui.

Palikę nuošalyje nukrypimą, susijusį su Cha0, turime pripažinti, kad labiausiai klestintys vagys iš Tamsiosios rinkos nepadėjo tvarkyti svetainės. Kalbame apie tokius vyrukus kaip Freddybb ir Recka, karderius iš Skantorpo ir Švedijos, kurie tik retkarčiais užsukdavo į svetainę verslo reikalais, o paskui dingdavo daugeliui dienų, savaičių ir netgi mėnesių. Teisėsauga visame pasaulyje suėmė

daug daugiau programišių entuziastų nei užkietėjusių nusikaltėlių, internetu atliekančių savo operacijas.

Plūkdamiesi tarsi vergai prie savo asmeninių kompiuterių, keturi aukščiausi Tamsiosios rinkos vadovai buvo atsakingi už keturias pagrindines sritis. Svetainės serverių apsauga ir bendra priežiūra buvo Meistro Splyntro ir Matricos atsakomybė. Kasdieniai grasinimai į svetainę ateidavo ne iš teisėsaugos institucijų, o iš Tamsiosios rinkos varžovų ir priešų, pasklidusių internetinėje erdvėje, pavyzdžiui, tokių kaip Ledo Žmogus. Splyntras, Matrica ir JiLsi dūsaudavo kas kartą, kai tarp narių kildavo ginčai. Splyntras prie to priprato, nors jį tai šiek tiek vargino. Paprastai vienas karderis galbūt nepagrįstai, o galbūt teisingai kaltindavo kitą kokiu nors pažeidimu. Apkaltintasis susirinkdavo savo žaislus ir netrukus įsižeidusioji konflikto pusė jau rikiuodavo kenkėjiškomis programomis užkrėstų kompiuterių tinklą, kad galėtų pradėti DDoS ataką. Dešimtims tūkstančių kompiuterių, kontroliuojamų vieno komandų ir kontrolės serverio, pareikalavus prieigos prie „DarkMarket“, svetainė būtų sunaikinta. Jei taip atsitiktų realiame gyvenime, burbėdavo Splyntras sau panosėje, tiesiog imtum ir iškarštum tam šunsnukiui kailį. Tačiau internete nėra didelės veiksmų pasirinkimo laisvės, todėl tenka uždaryti svetainę ir palaukti, kol puolimui pasiruošęs veikėjas aprims, arba vesti su juo derybas ir bandyti kaip nors susitarti.

Taigi administratoriai turėjo kontroliuoti visus tarp svetainės narių kylančius konfliktus ir mėginti juos sušvelninti, jiems dar neprasiveržus. Vidutiniam internetiniam nusikaltėliui būdingos šimpanzės manieros, o jo kalba panaši į žuvų pardavėjos Sicilijos turguje. Dėl anonimiškumo internete trūksta tarpusavio pasitikėjimo, o ypač tai pasakytina apie nusikaltėlius, kurie jaučia galimą policijos grėsmę ir suvokia nepažeidžiamumą, kurį naudotojui suteikia anonimiškumas. Tad įžeidimai tokiuose forumuose kaip „DarkMarket“ greitai perauga į atvirą žodinį karą. Tarp kitko, tai suteikia kozirį policijai, tiriančiai internetinius nusikaltimus – kai bendruomenė

susiskaldžiusi dėl įvairių įtarinėjimų, patyręs stebėtojas gali sumaniai manipuliuoti ginčais savo naudai.

Administratorių komanda, savaime suprantama, nulemdavo narių likimą „DarkMarket" hierarchijoje. Keturi nariai sudarydavo uždarą konklavą – slaptą forumą, kuriame galėjo dalyvauti tik jie. Jie, pavyzdžiui, nuspręsdavo, ar vogtų kreditinių kortelių pardavėjas pakankamai patikimai veda apskaitą, kad jam būtų galima suteikti patikrinto prekiautojo titulą, kuris jo turėtojui duos teisę pardavinėti korteles per Tamsiąją rinką be apribojimų.

Paprastai administratoriai nuolatos atidžiai tikrindavo svetainę, kad įsitikintų, jog į ją nepateko kibernetinė policija, jau nekalbant apie visokius niekšus ir plėšikus: banditus, kurie nepaklūsta nusikaltėlių pasaulio taisyklėms.

Plėšikų atpažinimas taip pat buvo svarbus ir trečioje, gyvybiškai svarbiausioje veiklos srityje. Ta veikla – tai sąlyginių įsipareigojimų paslauga, kurios tikslas – užtikrinti sąžiningą žaidimą nesąžiningoje sferoje. Kaip ir pirmoje kardingo svetainėje „CarderPlanet", sėkmingas sąlyginių įsipareigojimų paslaugos valdymas buvo svarbiausias veiksnys, kuris pavertė „DarkMarket" išskirtine šiuolaikine nusikaltėlių svetaine. Sąlyginių įsipareigojimų paslaugai vadovavo JiLsi, bet svarbiausias šios paslaugos arbitras buvo Cha0.

Galiausiai administratoriai turėjo atidžiai sekti, kad į svetainę nepatektų jokie veikėjai, kurie ja naudotųsi vaikų pornografijai platinti ar narkotikų ir ginklų prekybai. Tai buvo daroma ne iš moralinio pasipiktinimo, bet tikint, kad policija ne taip smarkiai persekios svetainę, jei ji apsiribos nusikalstama veikla su kreditinėmis kortelėmis ir tapatybės duomenimis.

Pirmąjį 2006 m. pusmetį Renu patyrė ir šilto, ir šalto. Nesėkmės prasidėjo nuo vasario. Sykį jis išėjo iš „Java Bean" kavinės, baigęs sunkius dienos darbus, svajodamas praleisti vakarą su „Martell"

taure ir kreko doze. Pabudęs kitą rytą pastebėjo, kad jo neįkainojamo atmintuko nebėra įprastinėje vietoje prie krūtinės. Jis bus palikęs tą prakeiktą daiktą kavinėje! Jį apėmė panika. Įėjęs į „Java Bean", jis nuskubėjo tiesiai pas šeimininką ir pasiteiravo, ar šiam kas nors nepadavė atmintuko. Šeimininkas papurtė galvą. „Per jus aš ką tik praradau ketvirtį milijono svarų!" – sušuko Renu, trumpam pamiršęs, kad tik jis pats yra kaltas dėl šios katastrofos. Jis mažiau sielojosi dėl savo ribotų lėšų nei dėl pinigų ir duomenų, kuriuos saugojo pagal sąlyginius įsipareigojimus.

Per kelias kitas savaites JiLsi surengė nuostolių patikrinimo operaciją. Juo pasitikinčius „DarkMarket" narius teko raminti, teigiant, kad jų saugumui nekilo pavojus. Tuo pat metu realiame pasaulyje Renu iš visų jėgų stengėsi laiku sumokėti paskolų įmokas už įkeistą nutriušusį nekilnojamąjį turtą šiauriniame Londone. Tamsioji rinka klestėjo, bet pats JiLsi nepraturtėjo. Priešingai, jis klimpo į skolas, taigi prašė kai kurių „draugų" paskolinti jam pinigų. Dezertyravęs iš interneto, jis būtų buvęs nepasiruošęs susidoroti su tradiciškesniu žemiškuoju „nusikaltėlių pasauliu".

Net praradęs savo atmintuką, Renu ir toliau išliko nesavanaudiškai atsidavęs Tamsiajai rinkai ir jos pažangai. Bet jį buvo apėmęs stresas, susijęs su svetainės valdymu. O svarbiausia, jis sužinojo, kad „DarkMarket" ir „CardersMarket" įsitraukė į mirtiną kovą. Svetainė buvo pažeidžiama, bet JiLsi buvo pažeidžiamas dar labiau, o kartais jis jausdavosi be galo pavargęs nuo visos šios aferos.

Padažnėjo Ledo Žmogaus puolimai, tarsi liūtimis užliejantys Tamsiąją rinką DDoS atakomis ir visokias kitokiais jam prieinamais ginklais. Viso pasaulio karderiai išsirikiuodavo į eilę tai prie vienos, tai prie kitos svetainės, įrodinėdami, kad priešininkai turėtų duoti kelią ir leisti dominuoti vienai svarbiausiai svetainei. Tai neabejotinai buvo pagrindinis Ledo Žmogaus argumentas: konkurencija nepadidina efektyvumo, o tik veda prie pykčių.

2006 m. rugsėjį negailestingos atakos varė Renu į nevilį. Tuo pat metu jo priklausomybė nuo kokaino jau tapo pastebima, o tai darėsi pavojinga tiek jo paties saugumui – jau nekalbant apie sveikatą, – tiek ir visos Tamsiosios rinkos saugumui.

Jis nusprendė pasikalbėti apie „DarkMarket" užpuolimus su Meistru Splyntru, kuris tuo metu buvo svetainės moderatorius, taigi dviem hierarchijos pakopomis žemiau nei pagrindinis administratorius JiLsi. Jau kuris laikas Meistras Splyntras įrodinėjo, kad JiLsi turėtų jam leisti perimti serverius. Kaminskis teigė, kad jis turi daug geresnių saugumo priemonių ir, jei perimtų serverius, tai sumažintų JiLsi pątiriamą spaudimą.

JiLsi Meistrą Splyntrą laikė atsarginiu variantu. Pirmiausia jis šį postą pasiūlė Cha0, bet turkas atsisakė, neabejotinai todėl, kad varginantis serverių priežiūros darbas jam nekėlė entuziazmo. Niekas kitas nenorėjo prisiimti atsakomybės, taigi JiLsi suprato, kad neturi kito pasirinkimo, kaip tik pakviesti Meistrą Splyntrą.

2006 m. spalio pradžioje, apie pusę dvyliktos vakaro, Kaminskis sulaukė skambučio. „Mano serveriai paruošti, JiLsi", – pasakė jis. JiLsi, ilgiau nedvejodamas ir laimingas, kad pagaliau gali perleisti atsakomybę už savo pažeidžiamus serverius, sušuko: „Tvarka. Tada pirmyn!"

Galbūt bijodamas, kad gali supykdyti savo draugužius administratorius, JiLsi nesitarė su jais, perduodamas serverių valdymą Splyntrui, nors neatrodė, kad kuris nors iš jų tam prieštarautų. Jie greitai patikėjo Splyntro išmintingumu – jis įrodė esąs geresnis šios paslaugos valdytojas nei JiLsi.

Kaminskis laikėsi žodžio: jo serveriai veikė efektyviai ir saugiai. Ir ne vien tai. Kai kas nors mėgindavo išsiaiškinti, kur iš tiesų yra Tamsiosios rinkos serveriai (ar tai būtų bičiuliai programišiai, ar teisėsaugos pareigūnai, karinės ar žvalgybos tarnybos), jų, paslėptų už anoniminio serverio Singapūre, niekas nesugebėdavo atsekti.

Meistras Splyntras buvo paskirtas administratoriumi. Į svetainę įeinančios ir iš jos išeinančios informacijos srautas vėl ėmė didėti. Kas kartą, kai Ledo Žmogus įsilauždavo į „DarkMarket“ svetainę ir sunaikindavo jos duomenų bazę, Meistras Splyntras per dvidešimt keturias valandas atkurdavo ją ir paleisdavo veikti. Ir nors Ledo Žmogus šiame žaidime neginčytinai buvo pats talentingiausias specialistas, jo arogancija atstūmė šimtus karderių. „DarkMarket“ vis stiprėjo, ir, regis, niekas negalėjo sustabdyti jos kilimo į aukštumas. Bet Ledo Žmogus turėjo atsarginį, paskutinį ėjimą.

18
Įtarūs protai

Išorinė Ledo Žmogaus ramybė slėpė tikrų tikriausią įtūžį. Jis prarado laiko pojūtį. Galėjo būti trečia nakties, o gal trečia popiet. Bet įsitraukus į labai svarbų darbą – įsilaužimą į kompiuterių sistemas, trunkantį valandų valandas, – nesunku buvo susipainioti. Patiems aistringiausiems programišiams laikas ir erdvė išnyksta. Kai Ledo Žmogų apėmė įtūžis, jis prarado tikrovės nuovoką – jam rūpėjo tik kerštо deivės Nemezidės įsakymai.

Ji pasirodė keliais pavidalais. Pirmasis buvo El Mariachi, susierzinęs karderis, kurio svetainę „The Grifters"* Ledo Žmogus buvo sunaikinęs. Pakilęs į skaitmenines aukštumas, El Mariachi šaukė turįs nepaneigiamų įrodymų, jog Ledo Žmogus realiame gyvenime bendradarbiauja su FTB. Jo kaltinimus atkartojo El Mariachi liokajus Lordas Cyrikas, amžinai viauksintis ir urzgiantis kardingo forumuose lyg kambarinis šunelis. Kaip ir daugelis kitų, Ledo Žmogus bjaurėjosi Lordu Cyriku.

Tulžingi kaltinimai buvo svaidomi iš vienos kardingo svetainės į kitą. Tai priminė kelių mafijos klanų karą, išskyrus tai, kad šiuo atveju niekas tiksliai nežinojo, kas kuriai šeimai priklauso, kas yra informatorius, o kas dirba Federaliniame tyrimų biure. Tvyrojo visiškas chaosas.

Tačiau kai Ledo Žmogus išsiaiškino tai, ką tuo metu palaikė tiesa, jis sėdėjo netekęs žado savo bute San Fransisko centre, už kurį

* *Grifters* – sukčiai. (Angl.)

mainais už nuolatinį vogtų kreditinių kortelių duomenų srautą mokėjo Jeffrey Normingtonas ir dar vienas partneris. Iš čia, apsikrovęs sužiedėjusiomis picos kriaukšlėmis ir kokakolos skardinėmis, Ledo Žmogus administravo svetainę „CardersMarket" ir liguistai brovėsi į kitas kardingo svetaines. Spalio mėnesį jam pavyko įsilaužti į pačią „DarkMarket" serverių širdį.

Jis pradėjo tyrinėti visus administratorių informacinius srautus ir pastebėjo kelis IP adresus, kurie jam pasirodė įtartini. Bet kas gali rasti IP adresus ir nustatyti jų buvimo vietą – išsiaiškinti, kokia kompanija ar individas su jais susiję ir kaip vadinasi jų interneto paslaugų teikėjas. Vienas adresas buvo įregistruotas kompanijos „Pembrooke Associates" vardu. Ledo Žmogus išnaršė visą internetą, norėdamas rasti informacijos apie šią kompaniją, bet niekur nieko nerado, išskyrus vieną svetainę su firmų sąrašais. Čia aptiko kompanijos pavadinimą ir jos telefono numerį. Tada atliko paiešką pagal telefono numerį ir rado kompanijos adresą: *2000 Technology Drive, Pittsburgh, PA.*

Užteko perskaityti adresą, kad net tokį veikėją kaip Ledo Žmogus nupurtytų drebulys. Tik prieš porą savaičių vyras jį buvo užtikęs, kai vienas jo kolega iš svetainės „CardersMarket" internete rado dokumento blanką, kuriame buvo įrašyta santrumpa NCFTA* ir tas pats adresas Pitsburge. Paieškojęs šios organizacijos, Ledo Žmogus išsiaiškino, kad tai Mokymų apie kibernetinių nusikaltimų įrodymus nacionalinis aljansas, pusiau vyriausybinė organizacija, padedanti įvairioms JAV teisėsaugos institucijoms dirbti su plataus diapazono internetinio saugumo klausimais.

Savo virtualios esybės gelmėse Ledo Žmogus staiga pajuto šaltą tikrovės prisilietimą. Jis visada įtarė, kad teisėsaugos atstovai tyko už kiekvieno kampo, tačiau šis atvejis buvo nedviprasmiškas – jis buvo

* *National Cyber Forensic Training Alliance.* (Angl.)

įsitikinęs, jog tai ne klaida. Daugelį mėnesių tikėjęs esąs neliečiamas ir valdąs kardingo bendruomenę, Maksas Vizija staiga sunerimo.

Po užsitęsusių konsultacijų trys Ledo Žmogaus kolegos iš „CardersMarket", prisidengę slapyvardžiais siloadmin, c0rruptedOne ir dystopia, nusprendė susisiekti su Matrica iš „DarkMarket" ir pasidalyti savo įtarimais apie IP adresą ir FTB ir suplanuoti tolesnius veiksmus. Matrica buvo vienintelis administratorius, kitų nuomone, niekaip nesusijęs su teisėsauga, taigi per „Icq" jie nusiuntė jam turimus įrodymus apie NCFTA ir adresą Pitsburge kartu su trumpa žinute:

dystopia: mes tai žinojom jau seniai, bet pagaliau turim įrodymų
dystopia: matrica, „DarkMarket" pakliuvo į spąstus
dystopia: šimtu procentų

c0rruptedOne: mes labai stengėmės išlaikyti taiką ir, jei išeisim į viešumą, teisėsauga mus KIETAI persekios, bet jei nieko nesakysim, būsim atsakingi už visus tuos, kurie bus apmauti

siloadmin: gerų dienų tau, į spąstus pakliuvusios svetainės administratoriau!
siloadmin: „Pembrooke Associates" Technologijos kelias 2000, Pitsburgas, PA 15219. Ar adresas Technologijos kelias 2000 tau nieko nesako?

Matrica įtarė kažką negero. Paprastai jis niekuo nepasitikėjo, bet ypač įtariai žiūrėjo į c0rrupted0ne ir siloadmin. Ilgą laiką „CardersMarket" veiksmai, nukreipti prieš „DarkMarket", dvelkė nežabota agresija, stengiantis visomis įmanomomis priemonėmis sužlug-

dyti svetainę. Jis patyrinėjo atsiųstą dokumentą ir, nors anglų kalba nebuvo jo gimtoji, iš karto pastebėjo, kad tekste knibždėte knibžda klaidų:

matrix001: „word" formato dokumentas padirbtas
matrix001: nejaugi, vyručiai, nė vienas iš jūsų nepastebėjot jame klaidų?
matrix001: o, ir jo antraštėje nėra kompanijos pavadinimo ar kokio kitokio pavadinimo, reiškiančio NCFTA
matrix001: tik adresas
matrix001: o, ir galiu paminėti bent vieną klaidą: rašoma „pasiekiamas", o ne „paseikiamas"
matrix001: vyručiai, ar man tęsti?

Siloadmin atsakė gindamasis, tarsi būtų supykęs ant savęs, kad nepastebėjo klaidų:

siloadmin: klausyk, matrica
siloadmin: suprantu, kad šitas šlamštas atrodo klastotė, tos klaidos ir visa kita
siloadmin: bet tai ištraukta iš interneto
siloadmin: ne aš sukūriau šitą šlamštą

matrix001: jokia kompanija visame pasaulyje niekada negalėtų turėti tokio firminio blanko
matrix001: tai visiškas absurdas

Visai galimas dalykas, kad tai buvo žabangos, o apsikeitimas žinutėmis būtent tuo ir įtikino Matricą. Konkuruojančių forumų apkaltinimas pakliuvus į teisėsaugos organizuotų operacijų pinkles buvo plačiai paplitęs metodas, siekiant atbaidyti jų narius prisidėti

prie konkurentų. Matrica buvo įsitikinęs – jei Tamsiosios rinkos nariai išeis iš jos, juos nedelsiant užverbuos Ledo Žmogus ir Karderių rinka, o tai galėtų sukelti grėsmę Tamsiosios rinkos egzistavimui apskritai.

Dar daugiau, siloadmin, dystopia ir c0rrupted0ne labai entuziastingai – gal net per daug entuziastingai – reikalavo, kad Matrica atidarytų kitą, suglaudintą *zip* formato failą, archyvuotą *rar* formatu. Kaip žinoma, *zip* formato failai – labiausiai paplitę trojanų užkrato nešiotojai, taigi Matrica buvo įsitikinęs, kad šį failą „CardersMarket" komanda sukūrė tam, kad iš jo kompiuterio išsiurbtų visas „DarkMarket" paslaptis. Jam pasidarė įdomu, ar Ledo Žmogus ir jo šutvė jau vykdo antrąjį etapą ryžtingo plano, kurį FTB sugalvojo, norėdama sunaikinti Tamsiąją rinką.

Vidurio Vokietijoje buvo šaltas lapkričio rytas, maždaug penkiolika po devynių. Matrica žinojo, kad reikia veikti greitai. Jis nedelsdamas susisiekė su savo bičiuliais administratoriais ir perspėjo juos, kad Ledo Žmogus ir jo gauja nusiteikę demaskuoti Tamsiąją rinką:

matrix001: aš neįsikėliau ir neatidariau failo, pasakęs, kad mano *rar* failų išarchyvavimo programa neveikia
matrix001: esu tikras, kad tai buvo trojanas
matrix001: jei patikrinsit jų atsiųstą informaciją, pamatysit, kad ji gana įtartina...
matrix001: bet paskaitykit patys...

19
Donnie Brasco

Pitsburgas, 2006 m. spalis

FTB Kibernetinių nusikaltimų skyriaus specialusis agentas Keithas J. Mularskis kraustėsi iš proto, bet ne tik todėl, kad Pitsburgo profesionalų futbolo komandai „Steelers" po sensacingos praeito vasario pergalės aukščiausio lygio čempionate šį sezoną nelabai sekėsi. Nors ir turėjo sezoninį bilietą į komandos „Steelers" „Heinz Field" stadioną, Mularskis visada pripažino, kad futbolas nėra gyvenimo ir mirties klausimas – jis dar svarbesnis nei gyvenimas ir mirtis. Bet šį sykį jis turėjo rimtesnių problemų nei futbolas.

Jau daugelį mėnesių jis dirbo, prisidengęs internetiniu slapyvardžiu Donnie Brasco, vis giliau nirdamas į nuolat besiplečiantį kriminalinių nusikaltimų liūną. Tiesa, jo gyvenimas niekada nebuvo atsidūręs tokiame pavojuje kaip FTB agento Joe Pistone'o, kuris, pasivadinęs Brasco vardu, slapta prasiskverbė į kiečiausias Niujorko mafijos šeimas. Bet Mularskiui teko atlikti daug pragariškai sunkaus darbo, norint gauti savo vadų sutikimą vykdyti precedento neturinčią slaptą operaciją internetinėje erdvėje. Ją buvo sunku paruošti, be to, grėsė didelis pavojus pakliūti į spąstus ir būti demaskuotam. Taigi FTB vadai sekė kiekvieną jo judesį, bijodami galimų klaidų. Nors tai, kas įvyko, nebuvo klaida. Tai buvo susidūrimas kaktomuša.

Laikas spaudė. Jis jau ilgai išbuvo neatpažintas ir beveik sutarė dėl kelių užsienio teisėsaugos organizacijų paramos savo ilgalaikei

strategijai, pagal kurią buvo numatęs įvykdyti daugybę įspūdingų policijos reidų visame pasaulyje. Jis sukūrė ir išugdė savo herojų, parinkęs jam vardą ir sugalvojęs biografiją, ir per nepaprastai trumpą laiką šis pramanytas veikėjas tarp daugelio internetinių vagišių visame pasaulyje spėjo virsti realiu asmeniu. Mularskis buvo visai arti kelių savo tikslų.

Dabar, kai kolega neapdairiai paliko kompiuteryje failą su Mokymų apie kibernetinių nusikaltimų įrodymus nacionalinio aljanso firminio blanko duomenimis, jis buvo išsigandęs dėl grėsmės šiai nepaprastai sudėtingai operacijai ir galimo jos demaskavimo bei žlugimo.

Tai buvo pirmas labai svarbus FTB įsiveržimas į internetinių nusikaltimų sferą. Iki tol internetiniuose tyrimuose dominavo JAV pašto inspekcijos tarnyba, bet visų pirma – JAV slaptoji tarnyba. 2004 m. tapo aišku, kad internetiniai nusikaltimai sudaro vieną iš sparčiausiai augančių pasaulinės organizuotos nusikalstamos veiklos sektorių. Vis daugiau organizacijų, institucijų ir pavienių individų buvo apgaunami, įsibrovus į jų kompiuterius. Didžiausią problemą sudarė kreditinės kortelės, nes daug jų buvo panaudota piktnaudžiaujant ar pavogta. Didelės kompanijos tapo pramoninio šnipinėjimo aukomis, kai tie patys programišiai, kurie užsiiminėjo sukčiavimu su kreditinėmis kortelėmis, pavogdavo jų komercines paslaptis ir parduodavo jas konkurentams. Bendrovės „Cisco Systems“* konkurentas iš Kinijos pavogė ir nukopijavo vieno iš jos pažangiausių serverių planus, – taigi galima teigti, jog net ir su kompiuteriais susijusios korporacijos nebuvo saugios.

Aplaidus požiūris į kompiuterių tinklų saugumą tiek vyriausybinėse organizacijose, tiek privačiame sektoriuje jau buvo pradėjęs gąsdinti Baltuosius rūmus, Kongresą ir Pentagoną. Dauguma vyriausy-

* Didžiausia pasaulyje kompiuterių tinklo įrangos gamintoja.

binių institucijų ir ministerijų arba nežinojo apie savo pažeidžiamumą, arba buvo taip priblokštos į juos nukreiptų atakų, kad paprasčiausiai sukišo galvas į smėlį, vildamosi, kad gal problemos paprasčiausiai išnyks savaime. Tačiau Pentagonas negalėjo taip elgtis. Jis įklimpo, mėgindamas susidoroti su atakų į apsaugos skyriaus kompiuterines sistemas pasekmėmis. Šias atakas organizavo programišių grupė „Titan Rain", susikūrusi Kinijoje ir siekianti išgauti visas suklasifikuotas paslaptis iš neprotingai išdėstytų kompiuterinių failų.

Didieji bankai vis dar negalėjo atsigauti nuo vadinamojo PVV (angl. *Pin verification value*) – PIN verifikavimo reikšmės pažeidžiamumo, kuris „Shadowcrew" gyvavimo laikotarpiu tokiems bankams kaip „Citibank" ir „Bank of America" kainavo dešimtis milijonų, pavogtų grynaisiais, ir nors jie išsprendė šią problemą, šimtai kitų bankų vis dar žarstė karderiams grynuosius iš bankomatų. Vienu žodžiu, tvyrojo sumaištis.

Nesunku padaryti išvadas. Netrukus didžiulės mokesčių mokėtojų pinigų sumos bus nukreiptos tarpusavyje susijusioms internetinio nusikalstamumo, kibernetinio pramoninio šnipinėjimo ir kibernetinio karo problemoms spręsti. Jokia save gerbianti teisėsaugos institucija nenorės atsisakyti savo dalies. Žvelgiant iš FTB pozicijos, JAV slaptoji tarnyba jau buvo persisotinusi, nes gavo tris ketvirčius sotaus biudžeto pyrago. Pirmaudama tarp kibernetinių policininkų ir vis dar tebesimėgaudama „Shadowcrew" išardymo šlove, JAV slaptoji tarnyba, savaime suprantama, troško apginti savo viršenybę ir šioje dar tik užgimstančioje srityje.

FTB, būdamas didžiausia ir galingiausia Amerikos teisėsaugos institucija, manė kitaip. Jo direktorius Robertas Muelleris labai troško imtis kibernetinių nusikaltimų visų pirma todėl, kad gautų tam finansavimą, bet taip pat ir todėl, jog pats prisidėjo prie FTB modernizavimo, siekdamas, kad biuras taptų daugiau krašto žvalgybos agentūra nei policijos pajėgomis. Mularskio planas buvo

ne tik suimti nusikaltėlius, bet ir surinkti informaciją. Šis esminis krypties pakeitimas padėjo išvengti kai kurių vyresniųjų pareigūnų prieštaravimų, o Mularskis, kuris savo reikalavimą pradėti drąsią slaptąją operaciją pagrindė nuostabiu jos pristatymu, gavo įgaliojimus ją vykdyti. Tad kai jį „užkabino" Ledo Žmogus, ties pražūties slenksčiu atsidūrė ne tik operacija „DarkMarket". Jei situacija pablogėtų, tektų atsisveikinti ir su ateityje numatytais mokesčių doleriais, o kartu su jais ir su realia FTB galimybe vykdyti kibernetines operacijas. Mularskio pečius užgulė sunki našta.

Pirma jo reakcija buvo nusivylimas. Jis pamanė, kad viskas baigta ir jo sunkiai dirbanti komanda turės paruošti valdžiai žeminantį pasiaiškinimą, o kai kurie iš vadų murmės: „Mes juk taip ir sakėm!" Tačiau viena iš priežasčių, kodėl FTB savo agentų mokymo programai pirmiausia pasirinko Mularskį, buvo ta, kad jis buvo sumanus stresinėse situacijose. Taigi užteko kelių minučių, kad jis apsispręstų be kovos nepasiduoti.

Mularskio šeimos likimas buvo panašus į daugelio kitų dvidešimto amžiaus Pitsburgo šeimų likimus. Jo proproseneliui 1892 m. pavyko persikelti iš Hamburgo į Baltimorę. Jis atkeliavo tik su doleriu kišenėje. Keithas gal ir buvo tipiškas amerikiečių berniukas, bet, kaip ir daugelio Europos miestų bendruomenių, o Mularskio atveju – lenkų bendruomenės, jo tautinė savimonė išliko stipri.

Vaizdingoje Pitsburgo pietinėje dalyje tarp kuklių medinių namukų, *art deco* stiliaus kino teatrų ir šokių salių išsibarstę daugelio slaviškų bendruomenių bažnyčios ir bendruomenių centrai: čekų, lenkų, serbų, slovakų, ukrainiečių ir kitų, kurias patraukė šis strategiškai geroje vietoje esantis vakarų Pensilvanijos miestas.

Andrijus ir Julia Warholos, rusinų* pora iš kaimiškosios šiaurės rytų Slovakijos, emigravo į Pitsburgą dvidešimto amžiaus pradžioje, o

* Rusinai – rytų slavų tauta, kalbanti rusinų kalba.

vėliau jų šeimoje gimė viena iš įtakingiausių dvidešimto amžiaus meno pasaulio figūrų, tik dailininkas nubraukė nuo pavardės paskutinę a.

Galingi plieno tiltai ir užrašai, siejantys miestą su Norfolku ir Vakarų geležinkeliu – tai tik pora dalykų, primenančių svarbų Pitsburgo įnašą į Amerikos dominavimą dvidešimto amžiaus pasaulinėje ekonomikoje. Šiuose fabrikuose pagaminto plieno liejiniai buvo naudojami šarvuotiems laivams, lėktuvams, automobiliams ir pramonės įmonėms visame pasaulyje. Praėjo ne vienas dešimtmetis nuo tada, kai juodi debesys, kuriais spjaudėsi plieną gaminanti hidra, paskutinį kartą buvo apgobę miestą tamsa, paskleidę nuodingų dalelių, kurios kadaise buvo didžiausio plaučių ligų paplitimo Jungtinėse Valstijose priežastis.

Smogas jau nebetvyro virš miesto, ir dabar Pitsburgas yra laikomas viena iš geidžiamiausių vietų gyventi visose Jungtinėse Valstijose. Saulė skaisčiai šviečia, ir po penkiolikos skurdo ir nuosmukio metų praeito šimtmečio paskutiniame dešimtmetyje miestas palaipsniui tapo moderniųjų technologijų pramonės centru Rytinėje pakrantėje.

Mularskis išvyko iš miesto devintajame dešimtmetyje, baigęs istorijos mokslus Djukeino universitete. Tuo metu nebuvo kito pasirinkimo. Jo tėvą galėtume laikyti Vilio Lomano* reinkarnacija. Mularskis vyresnysis, vienas iš pirmųjų, nukentėjusių nuo lemtingo suklupusio milžino nuosmukio, dirbo pardavėju, bet aštuntajame dešimtmetyje buvo atleistas ir negalėjo rasti kito darbo. Šeima jautėsi nesaugi. Jie gyveno iš Keitho motinos sekretorės uždarbio.

Keitho jaunystėje gyventojų skaičius Pitsburge sumažėjo trečdaliu. Jis neturėjo noro stebėti, kaip šis skaičius ir toliau mažės, taigi su savo naująja žmona išvyko į Vašingtoną. Priimtas į darbą pas

* Vilis Lomanas – amerikiečių dramaturgo Arthuro Millerio pjesės „Komivojažerio mirtis“ pagrindinis herojus, pagyvenęs pardavėjas, pasimetęs tarp apgaulingų vilčių ir iliuzijų.

stambų baldų mažmenininką, išplėtusį savo verslą visoje šalyje, Mularskis demonstravo puikius vadybininko ir pardavėjo gebėjimus. Iš pirmo žvilgsnio neatrodo, kad pardavimo vadybininko darbas galėtų turėti ką nors bendro su kibernetiniais nusikaltimais, bet metodai, kurių jis išmoko kompanijoje, padėjo tvirtus pagrindus jo, kaip FTB policininko, dirbančio prie kibernetinių nusikaltimų, darbui.

„Socialinė inžinerija" – menas įtikinti žmogų padaryti ką nors, kas, objektyviai vertinant, jo nedomina, – ir sudaro kibernetinių nusikaltimų esmę. Kaip, sukčių manymu, galima įtikinti numatytą auką atskleisti slaptažodį? Arba atidaryti elektroninį paštą, kurio žinutėje slepiasi trojanas? Netgi paprasčiausiai įsijungti kompiuterį?

Internetiniai vagys turi keletą akivaizdžių galimybių. Du išbandyti ir patikrinti metodai – tai nemokamas muzikinių failų parsisiuntimas ir pornografija. Seksualinės paskatos yra vienos iš galingiausių – tai natūralu, nes per visą žmonijos evoliuciją partnerio paieška dažnai pasirodydavo esanti rizikingas užsiėmimas. Mes pasiruošę smarkiai rizikuoti, kad patenkintume savo seksualinius troškimus, o tai greitai perprato kompiuterinių virusų gamintojai. Poros krūtų vaizdo dažnai pakanka norint suvilioti patiklų naivuolį paspausti nuorodą į objekto adresą, iš kurio į jo kompiuterį bus atsiųsta pragaištinga kenkėjiška programa. Geriausiu atveju naivuolis išvys paveikslėlį, nors tai menka kompensacija už visų savo kompiuterio paslapčių perdavimą kažkur toli esančiam beveidžiam kontrolieriui. Neatsitiktinai vieno iš sėkmingiausių elektroniniu paštu išplatintų virusų temos eilutėje buvo parašyta „Aš tave myliu".

Nors pardavimo vadybininkai ir nesiekia platinti virusų, jie, panašiai kaip ir internetiniai vagišiai, yra patyrę žmonių sielų inžinieriai. Jų darbas yra įkalbėti potencialius klientus investuoti pinigus į nenorimus ar nereikalingus daiktus. „Parduoti tai, ką turi, kokiam nors žmogui, kuris pats to nori – menkas biznis, – kartą pareiškė gangsterių karalius Meyeris Lansky. – Bet parduoti tai, ko tu neturi,

kam nors, kam to visai nereikia – štai kur biznis." Pardavimo vadybininkas mažų mažiausiai gali įkalbėti klientus pirkti brangesnes prekes. Taigi kai ką tik iškeptas agentas Keithas Mularskis buvo priimtas į naujai susikūrusį FTB Kibernetinių nusikaltimų skyrių, jis atsinešė vertingą turtą – sugebėjimą palenkti, įtikinti, nekaltai papokštauti, įsijausti į kitų poreikius, paraginti, privilioti ir sugundyti. Būdamas policininkas, jis turėjo ir įtikinamų nusikaltėlio savybių.

2000-aisiais Pitsburgas buvo neatpažįstamai pasikeitęs. Jis visada turėjo naudos iš milžiniškų filantropų palikimų. Visas miestas paženklintas tokių Amerikos pramonės gigantų, iškilusių pereinamuoju iš dvidešimto į dvidešimt pirmą amžių laikotarpiu, kaip „Carnegie", „Heinz" ir „Mellon" ženklais. Viena iš naujų investavimo sričių, atsiradusi po gamybos nuosmukio periodo – tai investavimas į kompiuterių mokslą ir technologijas Carnegie'io-Mellono universitete (CMU), kuris vertinamas kaip viena iš dvidešimties geriausių aukštojo mokslo įstaigų visame pasaulyje.

Įkurtas vieno iškiliausių švedų kilmės pramonininko Andrew Carnegie'io, universitetas iš pradžių buvo technikos mokykla, o 1967 m. susijungė su „Mellon" pramoninių tyrimų institutu. Niūriuoju laikotarpiu, kuris tęsėsi nuo 1980 m. iki praeito amžiaus paskutinio dešimtmečio pradžios, CMU studijavo Pitsburgo sąstingio priežastis ir tyrinėjo galimo jo atsigavimo būdus. Universitetas taip pat buvo gerai žinomas savo darbais kompiuterių saugumo srityje. Šalia Masačusetso technologijos instituto ir Silicio slėnio, Pitsburgas iškilo kaip nuostabus ir pažangus didelės Jungtinių Valstijų kompiuterių entuziastų karalijos miestas, kurio specialistai domėjosi saugumo problemomis.

Puikus CMU įvertinimas daug pasako apie naująjį Pitsburgą, o kartu ir apie 1997 m. jame susikūrusį Mokymų apie kibernetinių nusikaltimų įrodymus nacionalinį aljansą, ne pelno siekiančią organizaciją, gaunančią paramą iš bankų ir įvairių korporacijų ir

siekiančią suburti akademinės srities, privataus sektoriaus, teisėsaugos ir žvalgybos profesionalus dirbti didėjančio internetinio nesaugumo klausimais. Kaip tik todėl Keithas Mularskis naujojo tūkstantmečio pradžioje grįžo namo dirbti nepretenzingai atrodančiame biure su įstiklintu fasadu. Šio biuro adresas – Technologijos kelias 2000.

Įdėmiai žvelgdamas pro fasado langą ketvirtame aukšte, Mularskis suprato, kad iš esmės jis vienas yra atsakingas už šią FTB operaciją. Vyras dirbo su puikia komanda, bet būtent jis įtikino savo labai skeptiškai nusiteikusius viršininkus duoti jam leidimą veikti. Tai buvo susiję ne tik su FTB reputacija, bet ir su jų susirūpinimu dėl biudžeto dalies – juk tai buvo jo darbas.

Ir tada jis prisiminė tai, ką iš tiesų gerai išmanė: pardavimą. Arba, tiksliau pasakius, socialinę inžineriją.

Kai kriminaliniuose pranešimuose šmėstelėjo žinia, kad Tamsioji rinka priklauso Federaliniam tyrimų biurui, Mularskis aprimo, priminęs sau, kad savigaila dar niekam nėra padėjusi. Jis kreipėsi į Grendelį, galbūt paslaptingiausią iš visų Tamsiosios rinkos narių. Realiame gyvenime Grendelis dirbo visiškai legalioje aukštos klasės Vokietijos kompanijoje, bet tuo pat metu siūlė mokamas paslaugas įtakingiems kibernetiniams nusikaltėliams. Tamsioji rinka naudojosi jo virtualiu privačiu tinklu, kuris garantavo beveik absoliutų anonimiškumą, be to, Grendelis buvo taip pat sukūręs keturis „apvalkalus" – programinę įrangą, padarančią naudotoją iš tiesų nematomą.

Grendelis iš apvalkalų sugebėjo atgaminti ankstesnius prisijungimo vardus, bet nė viename iš jų niekur nebuvo minimas „Pembrooke Associates" pavadinimas. Visiems „CardersMarket" ir „DarkMarket" nariams Mularskis išdidžiai gyrėsi, jog VPN paslauga priklauso jam, o vienintelis asmuo, susidūręs su „Pembrooke Associates" prisijungimo vardu, yra... Ledo Žmogus. Pasinaudodamas savaisiais pardavėjo

metodais, keršto dievas Mularskis nukreipė prožektoriaus šviesą nuo savęs tiesiai Ledo Žmogui į akis.

Klaidos ant blanko su kompanijos rekvizitais, kurias pastebėjo Matrica, buvo tik žiedeliai. Buvo žinoma, kad Ledo Žmogus jau ne sykį beatodairiškai kaltino visus, kurie kada nors jį suerzino, o kol jis ėjo vadovaujamąsias pareigas Karderių rinkoje, vienu ar kitu atveju jį buvo suerzinęs vos ne kiekvienas. Jis turėjo labai mažai draugų. Be to, vėl paplito nuomonė, kad Ledo Žmogus iš naujo ėmėsi savo senų FTB konfidencialaus informatoriaus triukų – ir Mularskis ėmė energingai kurstyti šią tezę.

Užuot sužlugdęs Tamsiąją rinką, Ledo Žmogus pasiekė priešingą efektą. Ji iškilo stipresnė nei bet kada ir dabar buvo beveik visų pripažįstama kaip pagrindinė viso pasaulio kriminalinė kardingo svetainė anglų kalba. Greitas Mularskio mąstymas nukreipė realią grėsmę.

20
Klastingas planas

JiLsi buvo labai patenkintas. Karderių rinka ir Ledo Žmogus vis dar tebesilaikė ant kojų, bet svirduliavo nuo atsakomųjų smūgių, pasipylusių po pareiškimo, kad Tamsioji rinka pakliuvo į spąstus. Dauguma karderių dabar klaidingai tikėjo, kad į spąstus pakliuvo Karderių rinka, o Tamsioji rinka eina teisingu keliu. Taigi Tamsioji rinka vėl pradėjo augti, kol galiausiai jos narių skaičius pasiekė 2000.

Be abejo, visgi sklido gandai, kad galbūt tarp Tamsiosios rinkos administratorių viskas vyksta ne taip, kaip atrodo, bet šiame etape tarp karderių buvo tiek pat „gaujos gyvūnų", kiek tarp pirmųjų internetinių nusikaltėlių buvo „vienišų vilkų". Gauja nusisuko nuo Ledo Žmogaus ir perbėgo į Tamsiąją rinką.

Iki 2006 m. gruodžio Tamsioji rinka gyveno visavertį gyvenimą. JiLsi didžiavosi savo laimėjimais – pagaliau jis buvo gerbiamas Šeimos narys, vertinamas už pasiaukojamą ir efektyvų darbą. Jis buvo suformavęs puikią komandą: Matrica, Meistras Splyntras ir Cha0 buvo neprilygstami administratoriai, o visi svetainės nariai pasitikėjo jų Sąlyginių įsipareigojimų tarnyba. Štirlicas ir Lordas Cyrikas teikė paramą ir užtikrino patikimumą. Jie greitai pastebėdavo plėšikus ir sukčius ir be ilgų svarstymų susidorodavo su šiais atliekų rinkėjais, vos tik jie iškildavo iš interneto kanalizacijos. Tarp svetainės narių kas kartą buvo sudaroma vis daugiau sandėrių, o jų pajamos pradėjo artėti prie tų, kurias savo auksinėmis dienomis pasiekdavo „Shadowcrew" ir „CarderPlanet".

Praėjo daugiau nei dveji metai nuo tada, kai žlugo „Shadowcrew". Įsivyravo ramybė. „Vieniši vilkai", kurie dabar forumuose sudarė mažumą, niekada nenuvylė savo gvardijos. Jie rūpinosi, kad nebūtų apkaltinti. Recka, sukčių karalius iš Švedijos, skrupulingai vengė turėti reikalų su amerikietiškomis kredito ar debeto kortelėmis, nes tuo atveju būtų patekęs tiesiai į JAV teisėsaugos akiratį; su švedais ir kitais europiečiais jis galėjo susitvarkyti, bet buvo atsargus, kad nepakliūtų į akis amerikiečiams.

Tačiau daugelis karderių, ypač jaunesnių, aplaidžiai žiūrėjo į savo saugumą. Jie nesinaudojo šifruotėmis bendraudami per „Icq" ir nepalaikė reikalingo virtualaus privataus tinklo ir tunelinio efekto sistemų, kad nuslėptų savo IP adresus. O Pitsburge Mularskis nenuilstamai kaupė duomenų bazę, naudodamasis savo sukurta programa, kuria buvo galima kryžmiškai analizuoti pavienių karderių veiklą – jis skaitė jų pranešimus, atgamindavo jų prisijungimo prie „Icq" vardus ir IP adresus ir, kur buvo įmanoma, susiedavo juos su „E-Gold" sąskaitomis.

Skaitmeninės valiutos paslaugos „E-Gold" naudotojams nežinant, vyriausybinės institucijos turėjo visą prieigą prie šio nuo 2006 m. paplitusio mėgstamiausio karderių tarpusavio atsiskaitymo būdo apskaitos įrašų. Paskui Floridoje buvo suimtas paslaugos įkūrėjas Douglas Jacksonas, įtariant, jog ši paslauga buvo naudojama pinigams plauti. Tačiau gal tik keli internetiniai nusikaltėliai (jei apskritai tokių buvo) padarė kokias nors išvadas dėl „E-Gold". Rusai vengė šių vakarietiškų kompanijų, registruotų Belize, ir teikė pirmenybę maskvietiškoms, kurių negalėjo pasiekti Vakarų teisėsauga.

Sukaupęs daugybę įrodymų ir vis didėjant jų kiekiui, 2006 m. žiemos pradžioje Mularskis susisiekė su kelių Europos šalių policija. Jis kalbėjosi su Didžiosios Britanijos sunkių organizuotų nusikaltimų agentūra SOCA, Vokietijos federaline policija, o vėliau su regioninėmis pajėgomis Badene-Viurtenberge.

Jis taip pat susisiekė su neseniai Paryžiuje įkurta ir proziškai pavadinta institucija – Centriniu biuru kovai su nusikaltimais, susijusiais su informacinėmis ir ryšio technologijomis OCLCTIC (pranc. *L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication*). Čia jis buvo sutiktas gana šaltai. Paprastai Prancūzijos policija labai noriai bendradarbiauja su Jungtinėmis Valstijomis, ypač terorizmo ir internetinių nusikaltimų klausimais, bet Prancūzijoje vis dar giliai įsišaknijęs tradicinis įtarumas, su kuriuo žiūrima į JAV ir jų ketinimus Europoje. Bet kuriai vyriausybei, norinčiai įsiteikti JAV, kyla grėsmė prarasti rinkėjų balsus, taigi ji įspėja pavaldžias tarnybas, kad jos būtų apdairios palaikydamos santykius su Vašingtono agentūromis.

OCLCTIC vadovas Christianas Aghroumas manė, jog absurdiška, kad kas kartą, kai jis ar jo pareigūnai ieško tokios kompanijos kaip „Microsoft" pagalbos, rizikuoja sulaukti nepasitenkinimo ir iš anksto nuspėjamų policijos kaltinimų, esą jie sėdi Amerikos korporacijų kišenėje. Aghroumas žinojo, jog iš tiesų neįmanoma net pradėti kovoti su internetiniais nusikaltimais, nesusitarus dėl bendradarbiavimo su tokiomis kompanijomis kaip „Microsoft". Aiškiai reiškiantis mintis ir įžvalgiai analizuojantis užslėptus politinius pavojus, su kuriais gali susidurti tarptautinės policijos pajėgos, Aghroumas buvo susitaikęs su faktu, kad nei Prancūzijos politikai, nei visuomenė ničnieko nenutuokia apie internetinius nusikaltimus ir apie tai, ko reikia, norint juos įveikti. Atrodė, kad dauguma prancūzų įsikibę laikosi iliuzijos, kad tarptautinius nusikaltimus galima įveikti ar sustabdyti, neperžengus savo šalies ribų, ypač jei įtariamas nusikaltėlis nekalba prancūziškai.

Bet Mularskis patyrė dar didesnį sukrėtimą už tą, kurį gali sukelti gerai žinomas prancūzų nusistatymas prieš amerikiečius. Jis sužinojo, kad OCLCTIC jau keletą mėnesių dirba su JAV slaptąja tarnyba dėl atvejo, susijusio su... Tamsiąja rinka. Lygiagrečiai vyko

tyrimas, o jis apie tai nieko nežinojo. Dar daugiau, JAV slaptoji tarnyba nebuvo nusiteikusi dalytis informacija apie savo tyrimus. Prieš kelis mėnesius Slaptosios tarnybos Kriminalinių tyrimų skyriaus viršininkas buvo iškilmingai pareiškęs Kongresui, kad dėl glaudaus skyriaus bendradarbiavimo „su kitomis federalinėmis, valstybinėmis ir vietinėmis vykdomosiomis institucijomis... mes galime sudaryti plataus masto tinklą keistis informacija, ištekliais ir technine patirtimi". Jis pamiršo apie tai pasakyti komandai, tiriančiai Tamsiąją rinką, nes net FTB jie atsisakė pranešti, į ką nukreipė savo pastangas. Reikalai pradėjo komplikuotis tiek kibernetinei policijai, tiek ir kibernetiniams vagims.

Dauguma Tamsiosios rinkos narių tuo metu nekreipė dėmesio į teisėsaugą (išskyrus tuos, kurie bendradarbiavo su Mularskiu). Jiems labiau rūpėjo pribaigti Ledo Žmogų ir įtvirtinti svetainės viršenybę. JiLsi apsiėmė kirsti lemiamą smūgį. Jei jam pasisektų, tai būtų jo sėkmės valanda, o jo autoritetas gerokai sustiprėtų. Be to, jam buvo atsibodę nesiliaujantys Ledo Žmogaus antpuoliai, kurie užkraudavo daugybę nesibaigiančių papildomų darbų. O ir tulžinga retorika bei pats Ledo Žmogaus vardas jam jau ėmė įkyrėti.

JiLsi planas buvo paprastas. Jis atsidarė anoniminę elektroninio pašto dėžutę, iš kurios pasiuntė žinutes Ledo Žmogaus internetinių paslaugų teikėjui. JiLsi jį įspėjo, kad jo priglobtoji „CardersMarket" yra kriminalinė svetainė ir kad jos savininkai užsiima stambiais sukčiavimais su kreditinėmis kortelėmis. Kai Ledo Žmogus atrado pašto dėžutę, iš kurios buvo siunčiamos demaskuojančios elektroninės žinutės, jis pasinaudojo JiLsi slapyvardžiu MSR206 (taip vadinosi legendinis kreditinių kortelių klonavimo prietaisas, kuriuo naudojosi visi karderiai) ir – valio! – jam pavyko.

Ledo Žmogus išsiaiškino, kad JiLsi šmeižia jį jo paties internetinių paslaugų teikėjui. To nebuvo galima atleisti. JiLsi iš tiesų peržengė ribą, kurios joks (ne)doras karderis neturėtų pažeisti, kad

ir kokie prasti būtų tarpusavio santykiai: jis įskundė brolijos narį. Dar blogiau, buvo sugautas tai darant.

Ledo Žmogus šią žinią paskleidė toli ir plačiai. Netrukus ji pasiekė ir Cha0.

Dėl Ledo Žmogaus kaltinimų visi jautėsi šiek tiek įsitempę. Ar į šį reikalą įsivėlę federalai? Ir dar daugiau – jei taip, tai „kas, po velnių, dirba su jais?" – kaip pareiškė vienas iš Tamsiosios rinkos administratorių. Ledo Žmogus, Splyntras, c0rruptedOne ar Silo iš „CardersMarket"? O gal paslaptingasis „rusas" Štirlicas arba naujasis „DarkMarket" moderatorius Lordas Cyrikas? Ar dar kas nors?

Dų žmonės, kurių niekas iki šiol nebuvo apkaltinęs dirbant policijai, buvo Matrica ir JiLsi. Jiems retsykiais buvo prikišamas nekompetentingumas (ir ne be pagrindo). Bet kad dirbtų policijai? Niekada. Ledo Žmogus jau seniai žinojo JiLsi slapyvardį iš savo antpuolių. Bet dabar atrodė, kad jį žino visi. Kilo įtarimų, kad kažkokios trečiosios šalies atstovai į JiLsi mylimą atmintuką infiltravo trojaną, dabar valdo kiekvieną jo klavišo spustelėjimą ir taip sužino didžiausias „DarkMarket" paslaptis. O gal JiLsi yra visai ne tas, kuo dedasi... gal jis kaip nors susijęs su paslaptingąja kompanija iš Technologijos kelio 2000 – „Pembroke Associates"?

Likus kelioms dienoms iki 2006 m. Kalėdų, JiLsi, kaip visada, jungėsi prie „DarkMarket" svetainės, norėdamas patikrinti informacijos srautą. Jis jau ilgą laiką nebuvo prisijungęs, nes tvarkė savo realaus gyvenimo reikalus. Tą popietę jis grįžo į „DarkMarket". „Naudotojo vardas: *JiLsi*, – įvedė jis. – Slaptažodis: *MSR206*." Kompiuteris akimirksniu išmetė pranešimą: „Neteisingas naudotojo vardas arba slaptažodis." JiLsi tuojau pabandė dar kartą, manydamas, jog netyčia bus nuspaudęs ne tą klavišą. Rezultatas buvo tas pats. Jis vis bandė ir bandė.

Neliko jokių abejonių: JiLsi, Tamsiosios rinkos dvasinis vadovas ir vyriausiasis administratorius, buvo išmestas iš savo paties svetai-

nės. Apimtas panikos, jis pamėgino prisijungti prie www.mazafaka.ru. Nepavyko. Kita svetainė „The Vouched" – įeiti negalim.

Netrukus jį išpylė šaltas prakaitas. JiLsi niekada nebuvo patyręs tokio skausmingo nuopuolio. Iš jo buvo išplėštas visas jo gyvenimas – arba bent jau tas vienintelis dalykas, kuris jam iš tiesų turėjo prasmę. Jis buvo piktas, įžeistas ir prislėgtas. Kas tai padarė ir kodėl? Jis pasinėrė į anestezuojantį „Martell" ir kokainą. Vakare ir naktį skausmas atlėgdavo, bet jis atsibusdavo dar labiau kentėdamas nei dieną prieš tai.

Galiausiai JiLsi pavyko per „Icq" susisiekti su Cha0. Jis baigė pokalbį svirduliuodamas, svaigstančia galva. „Mes žinome, kad tu dirbai Skotland Jardui ir nusikaltimų, susijusių su moderniomis technologijomis, padaliniui, – pareiškė jam Cha0. – Tavo sprendimas įskųsti Ledo Žmogų galutinai tai įrodė. Mes žinome, kad dirbi su teisėsauga. Tu buvai išmestas iš visų svetainių."

JiLsi tylėjo netekęs žado. Viskas, dėl ko jis dirbo, dingo akimirksniu, ir dabar jis buvo žlugęs. Kas toliau? Kur dėtis? Neviltis ir tremtis, JiLsi, neviltis ir tremtis.

V dalis

21
Drono palikimas

Kalgaris, Alberta, 2006 metai

Nuo ankstyvos jaunystės skelbdamas reklamas „Shadowcrew" svetainėje, Dronas visada sulaukdavo šilčiausių atsiliepimų apie savo darbą. „Vakar popiet aš gavau iš Drono kreditinių kortelių informacijos nuskaitymo prietaisą („skimerį"), – parašė „DarkMarket" svetainėje vienas patenkintas klientas. – Vakarą praleidau jį bandydamas ir esu labai labai patenkintas. Dronas turi aukščiausios klasės gaminių, kurie tikrai verti sugaišto laiko ir išleistų pinigų."

Dronas laikydavosi žodžio. „Greitas atgabenimas. Saugi pakuotė", – tvirtino komentatorius. Bet Droną tokį populiarų padarė ne operatyvus prekių siuntimas. Klientus sugrįžti ir vėl ką nors pirkti skatino jo teikiamos aptarnavimo paslaugos. „O dabar apie klientų aptarnavimą. Man atrodo, kad būtent šioje srityje Dronas dirba tikrai šauniai. Jis reguliariai siunčia savo pirkėjams naujausią informaciją, o kai parašau jam elektroninę žinutę apie tai, kas mane domina, ar ko paklausiu, per dvidešimt keturias valandas visada gaunu atsakymą. Velniškai įspūdinga."

Daugiausia dėl interneto naudotojų teisių ir lūkesčių ir į kriminalinį pasaulį galiausiai prasiskverbė kultūra. Jei nusikaltėlį apsuktų

internetinis pardavėjas, būtų sunku susekti pažeidėją ir pritaikyti tradicinį metodą – fizinį smurtą – nepasitenkinimui dėl prasto aptarnavimo išreikšti. Taigi dabar ir nusikaltėliai, pardavinėjantys internetu nelegalias prekes, turi konkuruoti, siūlydami geriausias paslaugas.

Būdamas kito amžiaus, Dronas būtų greitai iškilęs į aukštumas. Jis metė mokyklą gal penkiolikos, bet savo verslininko gyslelę papildė kūrybiniais sugebėjimais. Kai tėvas išmokė jį žaisti internetinėje akcijų biržoje, jis atsitiktinai užtiko nusikaltėlių forumus ir 2004 m. pavasarį, būdamas dvidešimt ketverių, įsiregistravo į sėkmingiausią „DarkMarket" pirmtaką „Shadowcrew".

Bet labiausiai jo meistriškumas pasireiškė dėl įgimtų inžinerinių sugebėjimų. Iš pradžių jis išmoko projektuoti ir konstruoti nelegalius kortelių skaitytuvus, kurie tiko dviejų populiariausių tipų bankomatams visame pasaulyje. Tai buvo sudėtingi prietaisai, verti kiekvieno cento iš tų 5 000 dolerių, kurių Dronas prašė už vienetą (savaime suprantama, kad, perkant dideliais kiekiais, buvo siūlomos nuolaidos). Dronas ne tik atsakydavo į klientų klausimus, bet siųsdamas gaminį pridėdavo instrukcijas, reikalingą programinę įrangą ir nemokamą universalios jungties (USB) laidą.

Jo biblioteka taip pat liudijo apie rimtą požiūrį į darbą. Šalia tokių leidinių kaip *Dokumentų klastojimas ir kiti su sukčiavimu susiję nusikaltimai* (*Document Fraud and Other Crimes of Deception*), joje buvo *Hologramos ir holografija* (*Holograms and Holography*) ir knyga apie asmens tapatybės kortelių padirbinėjimo metodus *Vyro su įtartina asmens tapatybės kortele paslaptys* (*Secrets of a Back Alley ID Man*). Bet gal svarbiausia jo knyga buvo *Maskavimosi metodai* (*Methods of Disguise*). Kai Dronas užeidavo į vieną iš daugelio savo gimtojo miesto interneto kavinių tvarkyti pardavimo internetu ir rinkodaros reikalų, jis paprastai dėvėdavo juodą beisbolo kepuraitę ir juodą švarką. Bet užbėgdamas į paštą arba imdamas iš kortelės

pinigus, gautus už parduotą nelegalų skaitytuvą, jis mėgdavo dėvėti raudoną kepuraitę ir mėlyną neperpučiamą striukę.

Jungtinių Valstijų slaptoji tarnyba pirmiausia įsidėmėjo Droną kaip reikšmingą „Shadowcrew" asmenybę. Buvo žinoma, kad „Shadowcrew" administratorius CumbaJohnny – Slaptosios tarnybos informatorius. Bet Dronas nepriklausė CumbaJohnny virtualiam privačiam tinklui – pagrindinei priemonei, kuria Slaptoji tarnyba kontroliavo narių veiklą. Jis buvo ne Jungtinėse Valstijose, o ir šiaip nebuvo lengvas taikinys. Vadinasi, jis nebuvo ir prioritetinis asmuo. Tačiau Slaptoji tarnyba neužmiršo Drono. Priešingai, jie užmezgė su juo santykius.

Nors Slaptoji tarnyba yra jauna, palyginti su JAV pašto inspekcijos tarnyba, ji turi ilgiausią kovos su kibernetiniais nusikaltimais istoriją. JAV slaptoji tarnyba 1865 m. buvo įkurta ne tam, kad suteiktų ginkluotą apsaugą prezidentui (nors tokia buvo viena iš pagrindinių Kongreso reakcijų į prezidento McKinley'io nužudymą 1901 m.). Pirminis šios institucijos tikslas buvo išaiškinti, tirti ir patraukti baudžiamojon atsakomybėn kiekvieną pinigų padirbėją ir platintoją, ir šio tikslo tvirtai laikomasi ligi šiol. Netrukus po tarnybos įkūrimo Kongresas ją įpareigojo tirti ir finansinius nusikaltimus.

Prasidėjus Antrajam pasauliniam karui, pagal Breton Vudso susitarimą Jungtinės Valstijos tapo neginčijamomis vakarietiškos ekonomikos lyderėmis, o doleris – pasirinkta rezervine kapitalistinio pasaulio valiuta. Nors Sovietų Sąjunga ir Kinija nepripažino dolerio viršenybės, abi didžiosios komunistinės valstybės vis dėlto troško sukaupti kuo daugiau „žaliųjų". Pasaulyje, kuriame dauguma vyriausybių griežtai kontroliavo per savo sienas pereinančius užsienio valiutos srautus, visuotinis JAV dolerių populiarumas vykdant įvairius atsiskaitymus smarkiai didino potraukį juos padirbinėti.

To pasekmė – Slaptosios tarnybos operacijų internacionalizacija, atsakas į viso pasaulio sukčių ir vyriausybių siekį praturtėti patiems

arba pakirsti Amerikos galią, spausdinant dolerių banknotus. Kad ir kur būtumėte, skaitydamas šiuos žodžius galite beveik neabejoti, kad netoliese yra įsikūrę Slaptosios tarnybos žvalgai. Bet nors ši tarnyba turi ilgas rankas, vis vien yra užkampių ir skylių, kurių net ir ji negali pasiekti. Pavyzdžiui, praeito amžiaus paskutiniame dešimtmetyje po pasaulį pasklido „superdoleriai". JAV vyriausybės nuomone, šių nepaprastai kruopščiai pagamintų, bet visgi netikrų 100 dolerių kupiūrų paketai buvo atspausdinti Šiaurės Korėjoje – vienoje iš kelių valstybių, kurių vyrai juodais drabužiais negali pasiekti.

Apsaugoti nuo kulkos prezidentą ir medžioti padirbtus dolerius – gana sunkūs uždaviniai, bet 1984 m. Kongresas pareikalavo, kad Slaptosios tarnybos veikla būtų dar labiau išplėsta, įtraukiant į ją sukčiavimus su kreditinėmis ir debetinėmis kortelėmis, dokumentų padirbinėjimą ir kompiuterines apgavystes.

Per du tolesnius dešimtmečius ši organizacija, tam tikra prasme uždariausia Amerikos teisėsaugos institucija, suformavo pačias geriausias operatyvines pajėgas. Tačiau Slaptojoje tarnyboje dirba tik 6 500 žmonių. Palyginkite – FTB yra beveik 30 000 darbuotojų. Ne taip seniai JAV slaptoji tarnyba buvo prijungta prie Krašto apsaugos departamento, o tai sudavė smūgį jos išdidumui. Šiedvi institucijos nedraugauja. Sunku pasakyti, ar taip nutiko dėl Slaptosios tarnybos menkavertiškumo komplekso, ar dėl FTB pranašumo komplekso – galbūt yra šiek tiek ir vieno, ir kito. Šiaip ar taip, jas sieja priekabių ginčų istorija, kuri daro įtaką svarbiausiems darbiniams reikalams.

Sunaikinusi „Shadowcrew" Slaptoji tarnyba nusprendė palaikyti santykius su Dronu, kuris 2005 m. pabaigoje įstojo į „DarkMarket". Jo, nelegalių skaitytuvų pardavėjo, šlovė čia augo taip sparčiai, kad greitai jis įkūrė savo interneto svetainę www.atmskimmers.com. Daugelį mėnesių Slaptosios tarnybos Bafalo kontora plušėjo, mėgindama nustatyti nors apytikrę Drono buvimo vietą. Pardavėjas

naudojosi Izraelio elektroninio pašto paslauga „Safemail“, nes žinojo, kad ši kompanija užblokuoja siuntėjo IP adresą, vadinasi, žinutės gavėjas negali jo atsekti. 2006 m. sausį Slaptoji tarnyba galiausiai galėjo atsipūsti, kai „Safemail“ sutiko atskleisti Drono IP adresą, mat JAV slaptosios tarnybos reikalavimai pasiekė lėtapėdę Izraelio kriminalinės teisėsaugos sistemą. Kaip paaiškėjo, Dronas naudojosi daugybe kompiuterių, esančių įvairiose vietose Kalgario srityje, kuri yra naftingoje Kanados Albertos provincijoje.

Kalgario policijos tarnybos detektyvui Spenceriui Frizzelliui aštuoniolika tolesnių mėnesių buvo įtempti. Slaptosios tarnybos biurai Bafale ir Vankuveryje pateikdavo jam po vieną IP adresą, kurį gaudavo iš „Safemail“ kiekvieną kartą, kai slaptasis agentas apsikeisdavo su Dronu elektroninėmis žinutėmis. Šie adresai visada priklausydavo tai vienai, tai kitai interneto kavinei. Kol detektyvas Frizzellis nustatydavo tikrąją vietą, šaukštai, be abejo, jau būdavo po pietų. Iki tol, kol nebuvo pradėjęs dirbti su šia byla, detektyvas Frizzellis nė nenumanė, kad Kalgaryje yra tiek daug interneto kavinių ir kad jos tokios populiarios. Jam vis labiau ir labiau dingojos, kad ieško adatos šieno kupetoje.

Mėnesių mėnesius atrodė, kad Dronas renkasi interneto kavines be jokios sistemos. Vieną dieną staiga kur nors išlindęs, kitą dieną pasirodydavo už trijų mylių. Kartais visai dingdavo iš Kalgario, sukeldamas baimę, jog pranyko visam laikui. Bet jis visada grįždavo, ir po kelių mėnesių Frizzellis pasiekė didelį laimėjimą. Smaigstydamas vėliavėles žemėlapyje, jis pastebėjo, kad visos Drono lankomos interneto kavinės yra netoli Kalgario bėginio transporto stotelių, linijoje, jungiančioje Somersetą su Kroufutu. Jis taip pat įsidėmėjo dvi ar tris parduotuves, kuriose Dronas, atrodo, mėgo lankytis.

O tai reiškė jį turint pakankamai informacijos, kad galėtų prašyti sekimo komandos pagalbos. Jam iškilo įprasti klausimai, su kuriais susiduria viso pasaulio kibernetinė policija. Kas nukentėjo

Kalgaryje? Kokie yra su kriminaline veikla susijusios apyvartos įrodymai?

Frizzellis gavo įgaliojimus veikti, bet tik ribotam laikotarpiui ir su labai nedidele žmonių komanda. Paprastai, gavęs iš Slaptosios tarnybos pranešimą, kad Dronas įsijungęs internetą, jis nusitverdavo ką galėdamas iš biuro ir išvykdavo jo ieškoti kur nors palei bėginio transporto maršrutą.

Detektyvas iš Kalgario šį didvyrišką darbą dirbo daugiau nei metus, po truputį siaurindamas įtariamųjų ratą, kol įsitikino, kad atrado tą vyriškį. Bet jis nežinojo, kad jam pavyko nutverti tik vieną siūlo galą aiškiai rimtesnėje Slaptosios tarnybos operacijoje, į kurią buvo įsivėlęs ne tik Dronas, bet ir daugybė kitų veikėjų visoje Europoje. JAV slaptoji tarnyba susisiekė su Sunkių organizuotų nusikaltimų agentūra SOCA Londone ir su Centriniu biuru kovai su nusikaltimais, susijusiais su informacinėmis ir ryšio technologijomis OCLCTIC Paryžiuje. „Štai taip mes dirbame, – sakė Slaptosios tarnybos atstovas Edwinas Donovanas. – Mes iš tiesų labai stengiamės bendradarbiauti su viso pasaulio policija. Kreipiamės į organizaciją, dirbančią su tokios pat rūšies nusikaltimais, ir sakome jiems, jog esame nusitaikę į vieną ar kitą objektą – ir, be abejo, tokiais atvejais svarbiausia yra keistis informacija."

Taigi Slaptoji tarnyba dalijosi informacija su policijos pajėgomis Britanijoje, Kanadoje ir Prancūzijoje. Bet buvo viena agentų grupė, su kuria jie visgi to nedarė – tai jų kolegos iš FTB. Akivaizdi pagieža, tvyranti tarp dviejų JAV institucijų, kėlė painiavą tarp europiečių – juk galiausiai prancūzai dirbo su JAV slaptąja tarnyba, vokiečiai – su FTB, o britai mandagiai balansavo tarp jų abiejų. Tai iš tiesų atrodė gana ironiškai, nes vieninteliai žmonės pasaulyje, kurie žinojo, kad ir FTB, ir Slaptoji tarnyba yra nusitaikę į tą patį asmenį, o būtent į JiLsi, priklausė užsienio policijos pajėgoms – Sunkių organizuotų nusikaltimų agentūrai SOCA Londone. Reikalai dar

pablogėjo, kai SOCA pareigūnai suprato, kad dvi konkuruojančios Amerikos institucijos iš tiesų tyrinėja viena kitos slaptuosius agentus, įtardamos juos esant nusikaltėliais. Pagaliau vienas vyresniųjų britų valstybės pareigūnų atsargiai informavo aukštesniuosius pareigūnus Vašingtone, kad galbūt FTB ir Slaptoji tarnyba turėtų atidėti į šalį savo nesutarimus, bent jau tol, kol truks tyrimas.

22
Susimovei, vyruti

Badenas-Viurtenbergas, 2007 metai

Buvo malonus gegužės pradžios rytas, nors Matricai jis neatrodė pavasariškas. Išorinis pasaulis nutolo, o burna išdžiūvo, kai jis dar sykį permetė akimis elektroninio pašto žinutę.

> Tavo fiksuotojo ryšio linijos slapta klausomasi.
>
> Tave seka Jungtinės Karalystės, Vokietijos ir Prancūzijos farai... Slėpk įrodymus.
>
> Įspėk kitus... Farai žino, kad *matrix001* yra Detlefas Hartmannas iš Eislingeno...
>
> Turi tik dvi savaites, kol farai smogs Jungtinėje Karalystėje ir Prancūzijoje...
>
> Perspėk visus karderius, su kuriais gali susisiekti.

Ką tai reiškia? Nuo ko atėjo ši žinutė? Jis dar sykį pažiūrėjo į siuntėjo adresą – auto432221@hushmail.com. Ji galėjo būti sugeneruota atsitiktinai. O ir apie jos autorių jis nieko negalėjo pasakyti, išskyrus tai, kad jo anglų kalba buvo sklandi.

Matrica nusprendė pasitarti su savo bičiuliais Tamsiosios rinkos administratoriais ir pora kitų patikimų draugų. Jis paklausė, ką jie apie tai mano. Jie atsakė keistai ramiai, kai kuriais atvejais kone abejingai – tiesiog paprasti įspėjimai būti atsargiam.

Keithas Mularskis iš Pitsburgo dėjosi abejingas. Elektroninių žinučių ištraukos, kurias jis kartu su kitais gavo iš Matricos, reiškė tik vieną dalyką: informacija apie operaciją nutekėjo. Ir jeigu ji pasiekė Matricą, kas dar buvo slapta sekamas? Vargu ar tam galėjo būti netinkamesnis laikas, nes jau kelis mėnesius FTB planavo pirmąją Tamsiosios rinkos areštų bangą. Tvarkyti reikalus su nelinkusia bendrauti Slaptąja tarnyba jau ir taip buvo nelengva. Vokietijos policija iš Badeno-Viurtenbergo federalinės žemės buvo girdėjusi, kad jų kolegos iš Prancūzijos ruošiasi areštams, susijusiems su Tamsiąja rinka, bet prancūzų policija užgavo savo kolegas iš Vokietijos, sakydama, kad jų dalyvavimas planuojamame susitikime su Didžiosios Britanijos SOCA ir su Slaptąja tarnyba Paryžiuje nėra būtinas.

Matricai atsiųsta anoniminė „hushmail"* elektroninio pašto žinutė sukėlė tiriančiųjų policijos pajėgų susirūpinimą daugeliui mėnesių. Jiems reikėjo sužinoti, ar informacija nutekėjo dėl neatidumo, ar tai padaryta iš vidaus, o gal iš tiesų koks nors programišius prasiskverbė į tyrėjų komandų kompiuterinius tinklus. Kas kartą, kai atsitikdavo kas nors blogo, kildavo įtarimas, kad veikia kažkoks tarp jų esantis išdavikas. Bendra nuotaika nuo to tik nukentėdavo.

Mularskio pastangos koordinuoti pirmuosius areštus pasirodė nelengvos. Kiekvienas policininkas bijo, kad, suėmus tik vieną sukčių, žinia apie tai, kad vyksta kažkas blogo, pasklis po forumus kaip miško gaisras ir ieškomi subjektai paprasčiausiai išnyks. Štai dėl ko Slaptoji tarnyba tokia maniakiškai paslaptinga...

Lukterkit minutėlę, pagalvojo Mularskis, o gal štai iš kur nutekėjo informacija – iš Slaptosios tarnybos! Jis atidžiai apsvarstė galimus kaltininkus: a) Slaptoji tarnyba; b) kas nors iš dalyvaujančiųjų jo paties operacijoje, nors tuo labai abejojo: FTB saugumas buvo

* Nemokama internetinė elektroninio pašto paslauga, suteikianti šifruotų žinučių persiuntimo galimybę. Papildoma apsauga – paslėptas IP adresas žinutės antraštėje.

sustiprintas nuo tada, kai Ledo Žmogus atkreipė dėmesį, kad čia dalyvauja federalai; c) SOCA žinojo apie Matricą, bet britai visada mokėjo tylėti labiau nei dauguma kitų; d) ir dar vokiečiai – jis paprasčiausiai neturėjo pakankamai patirties, kad galėtų įvertinti vokiečius, nors buvo pastebėjęs šiokią tokią trintį tarp regioninių pajėgų Štutgarte ir Federalinės policijos tarnybos, esančios Vysbadene, už poros valandų kelio į šiaurę, – jos abi žinojo Tamsiosios rinkos istoriją. Mularskis niekuo negalėjo būti tikras.

Akimirkai spėliojimus teko atidėti į šalį. Mularskis skubėjo susisiekti su Franku Eissmannu iš vietinės policijos Štutgarte ir aptarti su Matrica susijusį tyrimą, kol jaunasis vokietis dar nepaspruko. Štutgarte buvo nuspręsta, kad jau pats laikas rimtai imtis bylos, ir Eismannas pateikė planuojamą Matricos suėmimo datą. Tai savo ruožtu sukėlė problemų Londono, Kalgario ir Paryžiaus policijai, kurios galiausiai susitarė susitikti Londone balandžio pradžioje ir pulti savo įtariamuosius tą pačią dieną – birželio dvyliktąją. SOCA vis dar jautėsi šiek tiek nepatogiai, nes Slaptoji tarnyba stebėjo JiLsi dar nuo „Shadowcrew" gyvavimo dienų. Jį suimti norėjo tiek FTB, tiek Slaptoji tarnyba.

Bet Matrica nepaspruko. Atvirkščiai, jo pokalbiai ir elektroniniai laiškai, kuriuos perimdavo vokiečių policija, rodė, kad „hushmail" žinutės jo visai neįbaugino. Galbūt sprendimas pagreitinti Matricos bylos eigą buvo pirmalaikis?

Gegužės 10 d., praėjus lygiai savaitei nuo pirmos žinutės, jis gavo antrą. Šį kartą ji buvo nuo auto496064@hushmail.com. Auto496064 atrodė šiek tiek nusivylęs:

> Vyruti, tu susimovei.
>
> Mūsų tinklas perdavė tau vokiečių karderių sąžiningą perspėjimą, o ką tu darai? Kalbiesi su tais mulkiais iš FTB!

Tu, prakeiktas kvaily, nusipelnei kalėjimo.

Visgi mes pasekėm bendravimą tarp FTB ir vokiečių vyruko, pasivadinusio Ledo Žmogumi. Jie ant tavęs užsiundė slaptą farą, kuris tik ir laukia, kol tu ką nors pirksi ar parduosi. Mes dar nežinom jo vardo. Bet tu galėtum mums padėti išaiškinti jo tapatybę.

Ir, po velnių, būk malonus: tol, kol nežinome, kas tas slaptas faras, nieko nepirk iš tų vyrukų.

Kadangi buvai toks velniškai protingas, jog išdavei FTB, kad mes žinom apie juos, jie gali smogti anksčiau! Panaikink visą informaciją iš savo namų kompiuterio, net jei, po velnių, ji yra užšifruota, ir naudokis tik interneto parduotuvėmis.

Matrica ėmėsi neigimo politikos ir nepaisė perspėjimo. Jis nusprendė, jog tai dar vienas žaidimas, panašus į tuos, kuriuos prisiminė iš Ledo Žmogaus aferos. Tačiau policija įsiuto. Šį sykį Detlefo Hartmanno kompiuterį sekantys pareigūnai perėmė elektroninę žinutę tuo pat metu, kai jis ją atidarė. Frankas Eissmannas (kurį paslaptingasis auto496064 klaidingai palaikė Ledo Žmogumi) negalėjo patikėti, kad kažkas kontroliuoja visus Tamsiosios rinkos ryšius. Pareigūnai ėmė baimintis, kad buvo įsilaužta į visą Tamsiosios rinkos tyrimą ir kad blogi vyrukai apie šią bylą žino viską, ką ir policija.

Mularskis taip pat buvo pritrenktas. Tačiau jis atkreipė dėmesį į vieną svarbią smulkmeną – anoniminės elektroninės žinutės siuntėjas galbūt iš tiesų puikiai mokėjo anglų kalbą, tačiau nebuvo amerikietis, nes žodį *favour* rašė su raide „u“*. Tai kas gi jis toks?

* Žodį *favour* – malonė, paslauga (angl.) britai rašo su „u“ raide, o amerikiečiai – be.

23
Kvadratinė matrica

2007 m. gegužės 29-oji. Eislingeno žmonėms antradienis tik prasidėjo. Eislingenas – viena iš nesuskaičiuojamos daugybės beveidžių Vokietijos bendruomenių, kur sugedęs šviesoforas ar pasimetusi karvė gali tapti didžiausia naujiena daugeliui mėnesių ir kur įprastinė rutina sutrinka retai. Gyvenimas Vokietijoje prasideda valanda ar dviem anksčiau nei Britanijoje ar Amerikoje. Pusę septynių ryto nenutrūkstamu srautu žmonės keliauja į darbą ir trumpam užbėga į vietinę „Tchibo" kavinę. Čia prie puodelio kavos, padengtos nepatrauklia kondensuoto pieno puta, kurią atperka grietininiai pyragėliai ar *Weggle* (taip sunkiai suprantamu Švabijos dialektu vadinama bandelė), jie trumpai pasikeičia paskalomis.

Kažkur H. gatvės viduryje Detlefas Hartmannas išsiropštė iš lovos, miglotai suvokdamas, kad turi prisiminti kažką svarbaus. Vis dar nelabai aiškiai protaudamas, jis patikrino savo „hushmail" elektroninį paštą, norėdamas įsitikinti, ar negavo kokių nors šifruotų žinučių, ir peržiūrėjo, ar nereikia ko nors patvarkyti savo interneto svetainėje, bet nerado nieko nepageidaujamo.

Tada jis prisiminė. Iš atostogų kaimyninėje Austrijoje turėjo sugrįžti tėvai. Reikia pasiruošti. Juodu su broliu turėjo tik vieną dieną apsikuopti. Lėkštės buvo aplipusios sudžiūvusiais spagečių likučiais tarsi kokiu pramoniniu cementu; peleninės su kalnais nuorūkų buvo netvarkingai išmėtytos tarp alaus skardinių, butelių ir neaiškios paskirties drabužių – tipiška likimo valiai paliktų paauglių aplinka. Detlefas nusprendė greitai nusiprausti, prieš imdamas tvarkytis, ir dar tik šluostėsi, kai sučirškė durų skambutis. Jis garsiai šūktelėjo į apačią broliui, kad atidarytų duris.

Detlefo susierzinimas, kad jį sutrukdė vos kelios minutės po pusės dešimtos ryto, dar padidėjo, kai brolis sušuko kažką apie siuntą, už kurią Detlefas turįs pasirašyti. Žirgliodamas laiptais žemyn, Detlefas pasiruošė ginčytis su paštininku, kad šis bus sumaišęs adresus. „Greičiau“, – nekantravo brolis, šiek tiek krūpčiodamas nuo skersvėjo, kol Detlefas artinosi prieškambariu.

„Tas automobilis pastatytas neleistinoje vietoje“, – pamanė Detlefas, metęs jam būdingą aštrų žvilgsnį ir pastebėjęs gatvėje stovintį juodą furgoną. Prieš jį stovėjo paštininkė. Ji vilkėjo uniformą, kurią Detlefas galėjo apibūdinti ne kaip kitaip, kaip tik išeiginę. Kaklaryšis buvo surištas mažu kietu mazgeliu, o ant galvos pūpsojo kepuraitė su standžiu snapeliu. Paštininkė atrodė labai rimtai.

Ji beveik nusilenkė, viena ranka paduodama Detlefui A4 formato voką, o kita – rašiklį. Kai jis ištiesė ranką paimti rašiklio, ji teatrališkai atsitraukė. „Kas, po velnių, čia vyksta?..“ – pradėjo Detlefas, bet nepabaigus sakinio ant jo užšoko keturi vyrai ir, pargriovę jį ant grindų, užlaužė rankas už nugaros. „Jūs suimtas!“ – suriko vienas iš jų, o tuo tarpu nežinia iš kur į namus įsiveržė dar keli pareigūnai. Detlefas gulėjo tik su pižamos kelnėmis. Lauke lijo ir buvo šalta, apie dešimt laipsnių šilumos pagal Celsijų. Kažkieno batas prispaudė jį prie šaltų grindų, o virvė, kuria jam buvo surištos rankos, įsirėžė į odą. Jis dar sykį sumurmėjo: „Kas, po galais, čia vyksta?“ – tarsi būtų užsikirtęs, vaidindamas antrarūšiame filme.

Po dešimties minučių jis sėdėjo priešais policijos pareigūną Franką Eissmanną iš Badeno-Viurtenbergo federalinės žemės. Pareigūnas rūškanu žvilgsniu įdėmiai žiūrėjo į maisto likučius virtuvėje, paauglių sukurto chaoso epicentre. „Viešpatie, kokia klaiki netvarka“, – pasibaisėjo detektyvas.

Detlefas paaiškino, kad tėvai išvykę atostogų. „Matyti“, – burbtelėjo Eissmannas sau panosėje.

Tada policininkas ir jo auka kelias minutes tylėjo. Tik Detlefas kaleno dantimis. Paradinės durys buvo paliktos atviros, tad kai lauke

lietus sustiprėjo, Detlefas visai sustiro. Nuo laiptų viršaus ataidėjo nekantrus riksmas: „Kompiuteriai vis dar veikia!“

Galiausiai Detlefas ėmė nutuokti, kas čia dedasi. Nepaisydamas šalčio ir sumaišties, jis mąstė greitai, taigi paklausė pareigūno, ar galėtų ką nors apsivilkti. Tai nebuvo visai nenuoširdu – jis iš tiesų šalo. Eissmannas dvejojo. „Gerai“, – sutiko jis ir įspėjo, kad tai visiškai neteisėta, bet jis vis dėlto leisiąs vyrukui apsirengti.

Einant į viršų, Detlefui galvoje kirbėjo vienintelė mintis. „Išjunk kompiuterį! Išjunk! Uždaryk jį! Uždaryk!“ – galvojo jis. Detlefas žinojo, kad policija neturi jo slaptažodžio, taigi jei jam pavyktų išvesti iš rikiuotės kompiuterį, neliktų jokių įrodymų. Jis samprotavo, kad tol, kol neturi slaptažodžio, jie neturi nieko.

Miegamajame Eissmanno kolega stovėjo priešais kompiuterį, susidėjęs rankas tarsi vartininkas, ir saugojo prietaisą. Vilkdamasis marškinėlius Detlefas parklupo ir, sugriebęs laidą su kištuku gale, ištraukė jį iš sienoje esančio lizdo. Gaudimas nutilo. „Šūdas, šūdas! – suriko pareigūnas. – Kompiuteris nebeveikia.“ Į kambarį įlėkė Eissmannas. „Tikrai taip. Tau pavyko, bet tai paskutinis dalykas, kurį padarei, ir ilgai daugiau to nebedarysi.“ Jis nutempė Detlefą laiptais žemyn į virtuvę. Eissmannas jam pakišo popieriaus skiautę su daugybe kanceliariniu stiliumi parašyto teksto, bet vienintelis dalykas, kurį prisimena Detlefas, buvo ranka pakeverzoti žodžiai: „*...įtariamas organizuoto kriminalinio sindikato suformavimu*“.

Nors buvo įsiutęs, detektyvas Eissmannas leido Detlefui trumpai pasikalbėti su broliu. Detlefas liepė jam nesinervinti, nes viskas bus gerai. Brolis nieko neatsakė, tik pažvelgė į jį, tarsi jis būtų visiškai kuoktelėjęs. Galiausiai, prieš išstumdamas Detlefą iš namų, Eissmannas paklausė, ar jis nenori ko nors pasiimti su savimi. „Ar galit patarti, kokių dalykų man gali prireikti? – klausimu atsakė apstulbęs Detlefas. – Nieko panašaus man dar niekada nebuvo atsitikę.“

Pakeliui į policijos nuovadą žvelgiant pro automobilio langą, jo mintys grįžo prie dviejų anoniminių elektroninio pašto žinučių,

kurias buvo gavęs prieš porą savaičių. Ką jis sau manė? Kodėl į jas nereagavo? Kad ir kiek stengėsi, Detlefas iš tiesų nelabai žinojo, ką konkrečiai būtų galėjęs padaryti. Jis nebuvo užkietėjęs nusikaltėlis, kuriam priklausytų namai su apsauga ir mafijos tinklas. Jis buvo tik jaunas ir gana naivus studentas. Vargu ar žinojo, kas yra tas kriminalinis sąmokslas, jau nekalbant apie tai, kad būtų prie jo prisidėjęs.

Detlefui vis dar apie visa tai mąstant, policijos automobilis atvažiavo į Štamheimo rajoną Badeno-Viurtenbergo sostinėje Štutgarte ir sustojo priešais didelį baltą pastatą Aspergerio gatvės gale. Jei būtų pažvelgęs aukštyn, viršutiniame aukšte būtų išvydęs langą tos kameros, kurioje 1976 m. pasikorė charizmatiškoji praeito amžiaus aštuntojo dešimtmečio Vokietijos kairuoliškos teroristinės grupės „Raudonosios armijos frakcija“ lyderė Ulrikė Meinhof.

Nuo tada Štamheimo kalėjimas tapo grynai vyriškas. Bet Detlefą į jį atvedė pareigūnė moteris. Kaliniai, vos pamatę moterį, įsisiautėjo, rėkavo iš savo kamerų nešvankybes apie tai, ką norėtų su ja padaryti.

Detlefo išgąstis dėl naujai susiklosčiusių aplinkybių augo sulig kiekvienu žingsniu. Kaipgi vaikinas iš padorios vidurinės klasės šeimos galėjo jaustis šioje situacijoje? Baigęs vidurinę puikiais pažymiais, jis ruošėsi studijuoti. Tėvai jį labai mylėjo ir buvo dėkingi už pagalbą prižiūrint tris jaunesnius brolius ir seseris. Dabar niekam žalos nepadaręs vaikinas iš Eislingeno atsidūrė Štamheime, liūdniausiai pagarsėjusioje įkalinimo vietoje visoje Vokietijoje. Nurengę ir apieškoję, kalėjimo prižiūrėtojai davė jam per didelius kalinio drabužius, bet nedavė batų. Jo naujoji pižama buvo tokia didelė, jog priminė žvejo kombinezoną. Buvo atneštas maistas, bet jis vis dar negalėjo įsisąmoninti, kad teks čia likti. Buvo ištiktas šoko. Palengva suprato, jog tai prieš penkerius metus prasidėjusios jo nedidelės kelionės galutinis etapas. Buvo praėjusi tik viena diena po jo dvidešimtojo gimtadienio.

24
Prancūziška jungtis

Marselis, 2007 metų birželis

Kadangi dvi JAV institucijos iš esmės nustojo kalbėtis, jos atskirai, bet vienu metu pradėjo Tamsiosios rinkos puolimą. Dalyvaujant Slaptajai tarnybai, detektyvas Spenceris Frizzellis Kalgaryje areštavo Droną keturiomis dienomis anksčiau, nei pietų Vokietijoje buvo atlikta FTB palaikoma operacija prieš Matricą.

Daugelį savaičių Frizzellis siaurino „įprastinių įtariamųjų" ratą, lankydamas nesuskaičiuojamą daugybę interneto kavinių, kuriose dirbo Dronas. Galiausiai jis išskyrė įprastinės išvaizdos dvidešimt šešerių vyruką, kuris vaikščiodamas darbiniais reikalais kas kartą keisdavo tris kasdienes „uniformas". Paieškos objektas gyveno gerame bute Kalgario centre, iš kurio, savaime suprantama, buvo patogu pasiekti miesto bėginį transportą.

Tačiau nei Frizzellis, nei Slaptosios tarnybos agentas nebuvo tinkamai pasiruošę tam, su kuo susidūrė. Įtariamasis Nicholas Joehle'as buvo pagaminęs apie šimtą nelegalių skaitytuvų. Visus juos pardavęs, jis būtų gavęs 500 000 dolerių grynųjų pajamų; taip pat jis turėjo šimtus tuščių plastikinių kortelių ir hologramų, paruoštų vogtai informacijai klonuoti. Be abejo, vien šių įrenginių turėjimas pats savaime nebuvo nusikaltimas, bet Frizzellis sugebėjo išsiaiškinti, kad per beveik dvylika tyrimo mėnesių Joehle'as parduodamas nelegalius skaitytuvus buvo užsidirbęs maždaug 100 000 dolerių.

Teisėsaugos institucijoms suimti asmenį, įtariamą nusikalstama veikla internete, yra vienas dalykas. Visai kas kita yra pateikti apkaltai reikalingus įkalčius. Dėl virtualios ir daugianacionalinės tokių nusikaltimų prigimties ypač sunku įtikinti kaltintoją imtis bylos, taip pat ir įrodyti nusikaltimą teisme. Už Jungtinių Valstijų ribų šioje dar embriono stadiją tepasiekusioje teisės srityje nuosprendžiai paprastai priimami trumpesniam laikui nei tradicinių nusikaltimų atvejais, vadinasi, policijos pajėgos priverstos daug investuoti, o rezultatai būna gana menki. Tačiau problema su tokiais kaip Dronas yra ta, kad kuo labiau jiems sekasi, tuo smarkiau jie sugeba nusiaubti vietinę ir pasaulinę ekonomiką. Potencialūs nuostoliai dėl tokių įgudusių operatorių kaip Dronas – milžiniški. Visgi pasaulyje egzistuoja dešimtys tūkstančių aktyvių kibernetinių nusikaltėlių ir greičiausiai tik maža jų dalelė kada nors bus sugauta.

Nors Joehle'as buvo nekalbus ir neišsilavinęs, jis, be abejo, buvo talentingas. Turėdamas verslininkiškų ir inžinerinių įgūdžių, jis tikriausiai būtų atsigavęs po teismo bylos ir įkalinimo. Savo patirtį jis jau buvo perdavęs kitiems Tamsiosios rinkos nariams, o šioji savo milžinišką nelegalių skaitytuvų verslą jau buvo išplėtusi pusėje pasaulio. Tačiau galų gale nei nuo Drono, nei nuo detektyvo Frizzellio nepriklausė vienas dalykas – greitis, kuriuo įgūdžiai perduodami tamsiaisiais interneto kanalais. O tai yra dar viena įtikinama priežastis, dėl kurios nacionalinės policijos pajėgos turėtų gerinti bendradarbiavimą su savo kolegomis užsienyje.

Kai Dronas ir Matrica buvo pašalinti, policijai reikėjo skubiai imtis kitų, kol Tamsiosios rinkos nariai nepastebėjo, kad jų nuolatiniai bendravimo partneriai staiga ir nepaaiškinamai dingo iš interneto. Šiuo požiūriu Slaptosios tarnybos padėtis buvo geresnė, nes Cha0, pasinaudojęs savo, kaip Tamsiosios rinkos administratoriaus, teise, jau buvo išmetęs Droną iš forumo.

O kol Dronas reiškėsi forume, Cha0 pasinaudojo valdžia, kad išgautų jaunojo inžinieriaus profesines paslaptis. Kai tik Cha0 ir jo komanda (nes Cha0 turėjo keletą bendrininkų) įgijo reikalingų įgūdžių, jis nutraukė Drono narystę lygiai taip, kaip buvo padaręs su JiLsi 2006 m. gruodžio mėnesį. Dronas daugiau negalėjo reklamuotis Tamsiojoje rinkoje, o kadangi dauguma kitų forumų Tamsiosios rinkos ir Karderių rinkos peštynėse buvo sunaikinti, jaunojo kanadiečio rinkodaros strategija tapo smarkiai suvaržyta. Nustūmęs iš kelio Droną, Cha0 itin stengėsi įkurti savo beveik monopolinį nelegalių skaitytuvų pardavimo tinklą.

Kadangi Dronas jau anksčiau buvo išmestas iš Tamsiosios rinkos, trys jo partneriai prancūzai – Theeeelas, gyvenantis netoli Paryžiaus, Lordas Kaisersose'as ir Kalouche'as iš Marselio – nepastebėjo, kad Spenceris Frizzellis jį izoliavo. Visgi Slaptoji tarnyba nežinojo, kada federalų palaikoma vokiečių policija suims produktyviausią Tamsiosios rinkos administratorių Matricą. O netikėtas jo pašalinimas iš forumo greičiausiai būtų sujaudinęs likusius Tamsiosios rinkos narius.

Švedijoje Recka išsyk suprato, kad teisėsauga pakilo į žygį. Jis kas dieną keisdavosi draugiškomis žinutėmis su Matrica ir nepatikėjo keista žinia, kurią šis netikėtai paskelbė 2007 m. birželio pradžioje. Matrica aiškino, kad jo mama pakliuvusi į rimtą avariją, taigi jis kurį laiką nesirodysiąs. Bet kuris patyręs internetinis vagišius iš karto būtų supratęs, kad policija sužinojo jo slaptažodį (taip ir buvo) ir kad ši žinia – tai tik klaidinantis manevras.

Lordas Kaisersose'as, Theeeelas ir visa jų kompanija, žinoma, buvo kitokie. Jie buvo prancūzai. Prancūzijos įnašas į internetinius nusikaltimus buvo specifinis. Prancūzų nusikaltėliai buvo tokie pat užkietėję prancūzakalbiai kaip ir visi kiti jų tėvynainiai. Prancūzų kalbos sergėtoja *Académie Française* su nerimu stebėjo tolygiai augantį anglų kalbos, kaip visuotinio žargono, paplitimą pasaulyje

praeito amžiaus paskutiniame dešimtmetyje. Tačiau ji buvo patenkinta, matydama, kad skaitmeniniame pasaulyje dauguma prancūzų programišių ir interneto fanatikų pasiaukojamai kovoja prieš anglų kalbą, pagrindinį kalbos užterštumo šaltinį.

Tai reiškė du dalykus: internetiniai nusikaltimai Prancūzijoje iš pradžių buvo grynai nacionaliniai – jie neperžengdavo savo valstybės sienų, kaip kad visur kitur pasaulyje. Šalis užbėgo už akių internetui, 1982 m. sukurdama labai efektyvią informacinę technologiją „Minitel", leidžiančią perduoti tekstą į vaizdo ekraną per įprastines telefono linijas. Dėl šios priežasties prancūzų supratimas apie informacines technologijas buvo daug pažangesnis nei daugumos likusio pasaulio. „Minitel" sistema, per kurią klientai galėjo susirasti reikiamus telefonų numerius, pasitikrinti banko sąskaitas, nusiųsti kam nors gėlių ar nešvankiai paplepėti, naudodamiesi *messageries roses**, buvo daug patikimiau apsaugota nuo programišių nei internetas, ir tai iš dalies paaiškina, kodėl Prancūzijoje internetas tik dabar pradeda nukonkuruoti „Minitel". Taigi prancūzai buvo labiau apsaugoti nuo pirmųjų virusinių internetinių atakų. Dar daugiau – palyginti nedaug prancūzų programišių leido laiką tokiuose interneto forumuose kaip „CarderPlanet", „Shadowcrew" ir „DarkMarket".

Antra, brukamų elektroninių žinučių srautas Prancūzijoje didėjo lėtai. O ir pelnas iš jų buvo daug mažiau viliojantis nei iš tų, kurias generavo anglų, ispanų, o pastaruoju metu ir kinų masinio elektroninio brukalo siuntinėtojai. Rinka tam paprasčiausiai per maža. Dar visai neseniai apie aštuoniasdešimt OCLCTIC pareigūnų nesivargino kontroliuoti kitose šalyse kylančios kibernetinės grėsmės (priešingai nei Prancūzijos karinės ir žvalgybos organizacijos, turinčios labai pažangias kibernetines pajėgas). Operacija „Lordas Kaisersose'as" (Marselio komanda) ir operacija „Kietasis diskas"

* Sekso telefonu paslauga.

(Dronas ir Theeeelas) savotiškai siekė padėti OCLCTIC agentams išaiškinti savo politiniams vadams, kodėl prancūzų policijai reikia efektyviau bendradarbiauti su tarptautine teisėsauga. Galbūt labiausiai stulbina tai, jog tada, kai OCLCTIC organizavo areštus, naudodama tuzinus ginkluotų pareigūnų, kurie suruošė atakas tam tikrais adresais Marselyje ir Paryžiuje, Prancūzijos spauda apie tai net neužsiminė. Nė vieno straipsnio.

Suėmusi Theeeelą, policija pasijuto priblokšta, kai išsiaiškino, kad jam tik aštuoniolika metų – jis buvo jauniausias iš visame pasaulyje sulaikytų Tamsiosios rinkos narių. Theeeelas įsitraukė į kardingą, nes jam trūko pinigų studijoms universitete. Štai kai kurios jaunos merginos supranta, kad niekaip kitaip nepajėgs susimokėti už studijas koledže, kaip tik retsykiais parduodamos savo kūną, tad nesunku nuspėti, kad jauni interneto fanatikai taip pat gali susigundyti pasididinti pajamas. Ir, kaip įsitikino Theeeelas, kai pinigai ima plaukti, atsisakyti šio įpročio būna sunku.

Iš pradžių prancūzų pareigūnai manė, kad Lordas Kaisersose'as priklauso prie vienos iš daugelio smulkių nusikaltėlių gaujų, kurių pilna Prancūzijos Odesoje – Marselyje, dar viename patraukliame uoste su nepakartojama savita kultūra (o kalbant apie Marselį – dar ir su pasakiška virtuve). Sekdami policininkai išsiaiškino, kad vienas iš Kaisersose'o bendrininkų Dustinas turi nuosavą restoraną valanda kelio už miesto ir užsiima nedideliais sukčiavimais.

Tačiau kai OCLCTIC pareigūnai kartu su Marselio policija suruošė reidą į įtariamojo Hakimo B. butą Marselio centre, jie suprato, kad Lordas Kaisersose'as priklauso prie aukštesnės lygos. Jie ne tik rado bute įvairiausių kompiuterinių įrenginių, – ir pats butas buvo įrengtas elegantiškai ir skoningai. Hakimas nebuvo gatvės banditas. Jis buvo talentingas programišius, o jo brolis Ali B., kaip paaiškėjo, dirbo skubių pašto siuntų pristatymo kompanijoje DHL. Nėra daug verslų, kuriuos kibernetiniai nusikaltėliai vertintų labiau

už tarptautinį kurjerių verslą. Turėdamas brolį Ali, dirbantį DHL kompanijoje, Hakimas niekam nepastebint galėjo naudotis daugybe įvairių būdų prekėms ir pinigams pristatyti tiek į Marselį, tiek ir iš jo. O tai buvo svarbu, nes Hakimas buvo vienas iš didžiausių kreditinių kortelių informacijos, gaunamos iš Ukrainos kardingo karaliaus Maksiko, prekeivių.

Per dvejus metus Maksikas buvo pardavęs Hakimui duomenis, nuskaitytus nuo 28 000 kreditinių kortelių. Jų vertė grynaisiais buvo apie dešimt milijonų dolerių. Padedamas savo komandos – Ali, Dustino ir dar kelių – Hakimas klonuotas korteles ruošėsi išsiuntinėti po visą pietų Prancūziją, kad jos būtų panaudotos ten esančiuose bankomatuose. Jis buvo atsargus ir niekada nesinaudojo jokiomis prancūziškomis kortelėmis, tik amerikietiškomis. Jei šį sykį JAV slaptoji tarnyba nebūtų kreipusis į OCLCTIC, Lordas Kaisersose'as nebūtų sugautas iki šių dienų – ir būtų buvęs daug turtingesnis.

25
Nematomas žmogus

Renukanthui atrodė, kad jis gali pradėti naują gyvenimą. Pašalintas iš Tamsiosios rinkos jis tris savaites sirgo depresija. Svetainė, kurią jis sukūrė iš nieko, buvo vienintelis dalykas, turėjęs jam prasmę, o dabar ją iš jo išplėšė. Kai 2006 m. žiemą pakeitė 2007 m. pavasaris ir Renu atsigavo nuo pirmojo sukrėtimo, jį palengva užvaldė keistas laisvės pojūtis. Jis suprato, kad gali mesti rūkyti kreką ir gerti. Jo smegenis temdęs rūkas ėmė sklaidytis ir jis vėl grįžo į sporto salę, norėdamas numesti šiek tiek svorio, priaugto viską nustelbusio Tamsiosios rinkos administravimo dienomis: per trumpą laiką iš plono kaip šakaliukas vaikinuko jis virto išpurtusiu storuliu.

Po kelių savaičių Tamsiosios rinkos administratoriams jis nusiuntė prašymą leisti sugrįžti į interneto svetainę. Jie taip ir padarė, tačiau atmetė jo prašymą sugrįžti į administratoriaus pareigas. Vietoj to jie suteikė jam unikalų – nors gal ir bereikšmį – garbingą garbės nario vardą.

Dabar Renu nebeturėjo galios valdyti svetainės narių likimų, bet ir toliau galėjo prisidėti prie sklandaus svetainės funkcionavimo. Vienas jos narys užsiiminėjo sukčiavimu su kreditinėmis kortelėmis variklių alyvos ir tepalų kompanijos „Texaco“ garaže, pietinėje Anglijos pakrantėje esančiame Portsmute. Kažkas įsirengė mini kamerą virš savitarnos parduotuvės kasos aparato. Buvo ne tik nuskaitomos kreditinės kortelės, bet ir filmuojami jų savininkai, įvedantys PIN

kodą. JiLsi nelaimei, vien tik norėdamas padaryti paslaugą kitiems svetainės nariams, jis sutiko būti Sąlyginių įsipareigojimų tarnybos pareigūnu. Ir dar blogiau – Renu paprašė kito svetainės nario slapyvardžiu Sockaddras išgryninti korteles Jungtinėse Valstijose. O Sockaddras buvo pagrindinis Slaptosios tarnybos agentas Tamsiojoje rinkoje.

Šiaip ar taip, JiLsi forume dalyvaudavo nebe taip dažnai – jo kardingo dienos ėjo į pabaigą. Nors vis dar reikėjo planuoti būsimą veiklą, jis buvo beveik tikras, kad atėjo laikas atsisakyti nelegalių darbų. Reikėjo išsikapstyti iš painiavos, į kurią buvo įklimpęs.

Šeštasis Renu pojūtis jam taip pat kuždėjo, kad vyksta kažkas keisto. Tarsi budrus elnias, pasirengęs sutikti pavojų, jis stebėjo, klausėsi ir stengėsi išgirsti menkiausią šlamesį. Jam atrodė, jog pastebėjo porą paskui jį sėlinančių gyvūnų. Sekdamas akies kraštelių, įsitikino, kad aplink „Java Bean" kavinę spiečiasi liūtų gauja. Taip pat jis atidžiai tyrinėjo dangų, ar nepamatys jame ratus sukančių grifų.

Ar tai buvo paranoja? O gal iškilo grėsmė, kad du lygiagrečiai tekantys Renu ir JiLsi gyvenimai susidurs? Vis dėlto geriausia buvo numatyti visas įmanomas pasekmes. Jis ilgiau nebegalėjo palaimingai gyventi, nepaisydamas akivaizdžių ženklų: per ilgai prie kavinės stovinčio automobilio, į ją užsukančių neaiškių, neįprastai apsirengusių nepažįstamųjų. Po poros savaičių, eidamas į „Java Bean" ir išeidamas iš jos, Renu ėmė keisti savo maršrutą. Jis neabejotinai turėjo draugiją. Jį persekiojo liūtai.

O grifai buvo mažiau organizuotos, bet ne mažiau grėsmingos komandos nariai, jie siuntė įspėjimus, susijusius su tam tikromis finansinėmis prievolėmis, kurias Renu buvo prisiėmęs po pražūtingo epizodo su atmintuku, įvykusio daugiau nei prieš metus. Dabar jie troško atsiimti savąją grobio dalį. Ar kuri nors iš šių grupių norėjo derėtis? Ar jam vertėjo vengti jų abiejų?

Prieš du mėnesius, praeitą kovą, Mickas Jamesonas buvo paskirtas vadovaujančiuoju JiLsi bylos pareigūnu. Daugiau nei pusę metų jo darbdavys – Sunkių organizuotų nusikaltimų agentūra SOCA – sekė JiLsi, remdamasi Keitho Mularskio pranešimu. Tiek JAV slaptoji tarnyba, tiek FTB jau ilgą laiką buvo nusitaikiusios į JiLsi, nes jis itin aktyviai reiškėsi beveik kiekvienoje veikiančioje kriminalinėje svetainėje (kartais netgi atrodydavo, kad jei JiLsi nėra kokioje nors svetainėje, vadinasi, ji iš tiesų ne kažin ko verta). Jo išskirtinis linksmasis avatara – piratas su raiščiu ant akies ir trikampe skrybėle – buvo nesulaikomas.

SOCA buvo vienintelė policijos agentūra, žinanti tiek apie FTB, tiek apie Slaptosios tarnybos operacijas, susijusias su Tamsiąja rinka, ir šios Didžiosios Britanijos pajėgos, nukreiptos prieš organizuotus nusikaltimus, savotiškai veikė kaip pasyvios taikdarės, bent jau stengdamosi užtikrinti, kad Lordo Kaisersose'o ir Theeeelo suėmimo data Prancūzijoje sutaptų su Matricos suėmimo data Vokietijoje ir JiLsi Anglijoje.

Sekimo komanda nuo vasario mėnesio buvo nukreipusi į „Java Bean" savo kameras ir klausymosi aparatūrą. Pareigūnai persekiojo Renu. Jie pastebėjo, kad jis susitinka su keliais žmonėmis ir dažnai kalbasi tamilų kalba. Taip pat buvo pastebėję jį perduodant grynuosius pinigus ir atmintukus kitiems žmonėms – šie pristabdydavo savo automobilius, o paskui vėl greitai nuvažiuodavo. Jie netgi susidūrė su kitu Tamsiosios rinkos nariu, kuris taip pat dažnai lankydavosi „Java Bean" kavinėje. Bet jiems reikėjo Renu. Su teleobjektyvu jie buvo nufotografavę jo kompiuterio ekraną. Vienas iš Jamesono kolegų buvo prasiskverbęs į Tamsiąją rinką ir tapęs eiliniu jos nariu, taigi jie galėjo kontroliuoti daugelį JiLsi siunčiamų žinučių. Be to, neįkainojamą informaciją jiems teikė Mularskis. Tačiau jie vis dar neturėjo nenuginčijamų įrodymų, kad Renukanthas Subramaniamas ir yra JiLsi. Tam jiems būtų reikėję jį suimti.

Įvairios policijos pajėgos nusprendė imtis žygių prieš jį antrą birželio savaitę. Galiausiai buvo pasiektas tam tikras Slaptosios tarnybos ir FTB susitarimas – pradėti operaciją birželio 12-ąją. Šį planą sužlugdė Matricai pasiųstos anoniminės elektroninio pašto žinutės. Jei JiLsi areštas nepavyktų, labai tikėtina, kad žinia per kelias minutes pasklistų po visą Tamsiąją rinką ir daugelio kruopštaus pasiruošimo metų darbas nueitų perniek.

O tada išsipildė didžiausia Jamesono baimė – praėjus porai dienų po Matricos suėmimo, JiLsi kažkur pradingo niekam nepranešęs. Vieną rytą jis žygiavo ne į „Java Bean" kavinę, bet į netoliese esančią Vemblio parko metro stotelę, iš kurios metro traukiniai važiuoja į Londono centrą. Praėjęs parduotuvę IKEA, esančią prie Šiaurės aplinkkelio – eismo spūsčių varginamo Londono miesto žiedinio kelio, – JiLsi pastebėjo keistos išvaizdos vyriškį. O gal tai buvo moteris? Jis negalėjo nuspręsti. Gal geriausia tą žmogystą apibūdinti kaip dvilytį? JiLsi keliavo toliau Vemblio parko pusėn. Eidamas požeminės perėjos prie metro stotelės link, ant viršuje esančio tilto JiLsi išvydo ilgaplaukį vyriškį, kuris nenuleisdamas nuo jo akių kalbėjo telefonu.

Įšokęs į metro traukinį, važiuojantį „Jubilee" linija į miestą, prie Žaliojo parko JiLsi perėjo į Pikadilį, o galiausiai išlipo Lesterio skvere, bet, kaip atsitinka daugeliui žmonių stotyse, išėjo ne ten ir turėjo dukart grįžti, kol pasiekė skverą.

Jam nutirpo širdis: ten jau buvo misteris Dvilytis. O eidamas per Lesterio skverą, pilną turistų ir gatvės artistų, Renu beveik atsitrenkė į misterį Ilgaplaukį. Abejonių neliko – jį tikrai sekė.

Renu įpuolė į kinų restoraną ir kažką nutvėręs godžiai prarijo priešpiečiams. Išlindęs į saulę, nusileido Šv. Martyno gatve, siaurėjančiu keliu, virstančiu gatvele palei Nacionalinę paveikslų galeriją, o tada priėjo Trafalgaro aikštę.

Sukinėdamiesi aplink Nelsono koloną, lankytojai žavėjosi įspūdinga daugiau nei trijų su puse metro aukščio skulptūra, pastatyta

ant Ketvirtojo cokolio*, kur eksponatai keičiami maždaug kas aštuoniolika mėnesių. Skulptūra „Alison Lapper nėščia" vaizdavo britų menininkę Alison Lapper nuogą ir besilaukiančią. Lapper gimė be rankų, ir sprendimas pastatyti šią skulptūrą tuo metu sukėlė daug triukšmo. Skulptūra traukė minias, ir, Renu bandant prasibrauti pro turistų antplūdį, jo saugotojai yrėsi per minią paskui jį. Jis įšoko į pirmą pasitaikiusį autobusą ir užlipo į viršutinį aukštą. Kai autobusas įsuko į Šv. Martyno gatvę, Renu pažvelgė žemyn pro antro aukšto langą ir sugavo misterio Dvilyčio ir misterio Ilgaplaukio akis, bevil-tiškai besižvalgančias aplink ir ieškančias pasprukusio grobio.

Renu pranyko. Bet pranyko ne vienas, o kartu su JiLsi, paskelbęs savo paskutinį pranešimą internete.

Po poros savaičių Renukanthas ėjo link vieno iš kelių nekilnojamojo turto objektų, kuris, jei ir nebuvo jo nuosavas, tai bent jau tikrai buvo jo įkeistas. Beveik pasiekęs namą, stovintį visai prie Hitrou oro uosto nusileidimo tako, išgirdo skambant telefoną. Skambino tenai gyvenantis bičiulis, norėdamas perspėti Renu nesiartinti. Policininkai ką tik buvo įsiveržę į namą, mojuodami arešto orderiu.

Mickas Jamesonas, vadovaujantysis SOCA pareigūnas, tiriantis JiLsi bylą, jau buvo apsilankęs name pagrindiniu Renu adresu Koniston Gardense, taip pat ir keliuose kituose. Be savo darbo Tamsiojoje rinkoje prisidengus JiLsi slapyvardžiu, išeivis iš Šri Lankos taip pat sukčiavo su nekilnojamuoju turtu. Jis nuolatos meluodavo apie savo profesinę ir finansinę padėtį, siekdamas gauti paskolų iš kreditorių įvairiam nekilnojamajam turtui šiauriniame, vakariniame ir pietiniame Londone. Britanijos neužplūdo tokia kone visa apimanti karštinė, kokia apėmė finansų pramonę Jungtinėse Valstijose.

* Ketvirtasis cokolis – tai tuščias cokolis Trafalgaro aikštėje, ant kurio turėjo stovėti raitelio statula. Daugiau nei 150 metų buvo daug ginčijamasi, ką su juo daryti. XX a. pabaigoje buvo sudaryta komisija, kuri galiausiai nusprendė ant jo laikinai eksponuoti meno kūrinius.

Vis dėlto liūdnai pagarsėjusi savarankiško vertinimo sistema, pagal kurią jūsų žodis buvo laikomas pakankamu jūsų pajamų įrodymu, kartu su nusistovėjusia praktika skolinti sumas, iki penkių kartų viršijančias paskolos prašytojo metinį atlyginimą (nuosaikesnio skolinimo laikais šis skaičius niekada neviršydavo trijų), reiškė, kad sukčiauti įkeičiant turtą Jungtinėje Karalystėje buvo palyginti nesunku. Rinka buvo tokia konkurencinga, kad žiūrėti pro pirštus tapo geriausia bankininkystės praktika.

Tačiau po telefono skambučio Renu labiau parūpo įveikti tuos gilius vandenis, į kuriuos buvo paniręs, nei galvoti apie smulkias įvairių savo suktybių detales. Jis iš karto nusprendė eiti į pogrindį. Tris savaites prastai miegojo, vengė visų adresų, kuriuos įtarė esant vienaip ar kitaip sekamus. Tuo metu, kai gavo įspėjimą apie policijos reidą, jis turėjo apie 500 svarų.

Ir anksčiau Renu gyvenimas buvo karštligiškas ir rizikingas, bet jam visada patiko toks šiek tiek vaiduokliškas egzistavimas: niekada negyventi ilgai vienu adresu, vogčiomis perdavinėti atmintukus įtartinos išvaizdos bendrams ir, be abejo, būti garbinamu kardingo svetainių meistru, kai niekas nežino, kas tu esi iš tiesų. Iš pradžių jam atrodė, kad miegojimas kartono dėžėse po arkomis su alkoholikais tik padidins tokį paslaptingumą. Bet kai baigėsi pinigai, o gyvenimas pablogėjo tiek, kad teko gyventi beveik pusbadžiu, Renukanthas Subramaniamas – bejėgis, apsileidęs ir negaluojantis – nusprendė, kad bėgimas ir slapstymasis atves į aklavietę.

2007 m. liepos 3 d. jis įėjo į Vemblio parko policijos nuovadą ir pasidavė. Lengvoji operacijos „DarkMarket“ dalis buvo baigta.

Tarpinis epizodas

Man nežinoma nežinia kur esanti šalis

Talinas, Estija

Prieš keturias dienas iki oficialios visuotinių rinkimų balsavimo dienos 2007 m. pavasarį mažytė Baltijos šalis Estija, kurios gyventojų skaičius tesiekia 1,25 milijono, pirmą kartą pasaulyje pasiūlė savo piliečiams galimybę parlamentiniuose rinkimuose atiduoti savo balsą, neatsitraukiant nuo asmeninio kompiuterio. Jei eksperimentas pavyktų, po ketverių metų, 2011-aisiais, galiausiai būtų siekiama apsiriboti vien „virtualiais rinkimais".

Ant kortos buvo pastatyta daug. Jei Estija atliktų šį reikšmingą šuolį į skaitmeninę ateitį, neužtektų tik veikiančių sistemų, jos taip pat turėtų būti apsaugotos nuo išorinių atakų. Prieš metus Estija buvo oficialiai pripažinusi savo Reagavimo į kompiuterinio saugumo incidentus grupę (RKSIG), kurios pagrindinis darbas buvo reaguoti į bet kokius pažeidimus (ar jie būtų atsitiktiniai, ar piktavališki) internetiniame domene, turinčiame šios šalies priesagą „.ee". Tai apima nuolatinį į šalį įeinančios, aplinkinės ir išeinančios internetinės informacijos tikrinimą, siekiant išvengti įvairių anomalijų.

Žmogaus, atsakingo už visos šalies kompiuterių saugumą, vardas garsiai netariamas. Tai Hillaris Aarelaidas, iš išvaizdos panašus į tokį, kuris ką tik nenoromis išlipo iš lovos. Jis gali jums pasirodyti išsiblaškęs, bet iš tiesų šis žmogus yra atsidavęs savo reikalui, o tai padėjo jam iškilti iki vadovaujančiųjų Estijos policijos pareigūnų, nors pradėjo kaip eilinis eismo reguliuotojas. „Bet man labai patiko kompiuteriai, taigi pirmiausia mane pervedė į Taliną, o galiausiai buvau paskirtas visos šalies teisėsaugos vyriausiuoju už informaciją atsakingu pareigūnu." Dar vienas dalykas – jis neabejotinai panašus į kompiuterių fanatiką ir visiškai nepanašus į policininką (išskyrus tuos nuo devintojo dešimtmečio pasitaikančius atvejus, kai jam tenka tapti slaptuoju pareigūnu, kovojančiu su narkotikais), taigi galbūt viena iš priežasčių, kodėl jis 2006 m. perėjo į RKSIG, buvo susijusi su policininko uniforma.

2007 m. virtualių rinkimų dieną RKSIG ir buvę Hillario kolegos iš teisėsaugos buvo labai budrūs. „Kaip ir tikėjomės, – paaiškino jis, – pastebėjome, kad kažkas paleido autonominį rinkimų sistemos skenavimą." Atrodo, kad kažkas pasiuntė automatinio zondavimo programą, rinkimų serveriuose turinčią ieškoti prievadų, kurie per klaidą buvo palikti atviri. „Tai nebuvo labai rimta, nes autonomines skenavimo programas nesunku nustatyti, – aiškino Hillaris, – visgi tai sudarė realią grėsmę saugumui."

Tada jis susiėmė – tiek, kiek toks atsipalaidavęs žmogus kaip Hillaris gali susiimti, – ir išdidžiai paskelbė: „Praėjus penkiolikai minučių po to, kai pirmą sykį pastebėjome autonominę skenavimo programą, policininkas jau beldėsi į duris tam tikru adresu penkiasdešimt kilometrų į pietus nuo Talino esančioje Raploje ir klausė ten gyvenančio žmogaus: „Kam jūs paleidote autonominį rinkimų kompiuterių sistemos serverių skenavimą?"

Internetinio saugumo pasaulyje penkiolika minučių nuo piktadarybės nustatymo iki pareigūno atvykimo į kompiuterio, iš kurio

buvo įvykdyta piktadarybė, buvimo vietą, yra daugiau nei įspūdinga – tai nuostabu. „Mums pasisekė, kad atlikome tokį gerą darbą, – pasakė Hillaris, – nes pirmai didelei atakai, įvykusiai balandžio pabaigoje, buvome gerai pasiruošę."

Tikroji „didelė ataka", įvykusi praėjus porai mėnesių po rinkimų, Estijai buvo kitas kibernetinis „pirmas kartas", nes ji patyrė ilgalaikį internetinių tinklų puolimą, galiausiai privertusį ją nutraukti savo internetinius ryšius su išoriniu pasauliu. Kai kas teigia, jog tai buvo pirmasis kibernetinio karo atvejis.

Aš ieškojau Hillario po mėnesio nuo savo vizito į Silicio slėnyje įsikūrusią „Google". Iškeliavau į rytus ir nuvykau į Taliną. Šis gražus miestas yra labiausiai į šiaurę nutolusios Baltijos valstybės Estijos sostinė. Senamiesčio siena juosia turtingą skandinaviškos, vokiškos ir slaviškos architektūros paveldą. Šie stiliai atspindi Estijos kaimynų iš šiaurės, rytų ir vakarų buvusius imperinius siekius; tačiau šiek tiek daugiau nei prieš dvidešimt metų sugriuvus komunistinei santvarkai galiausiai čia įsigalėjo vietinė Estijos kultūra (nors rusai iki šiol sudaro beveik ketvirtadalį gyventojų).

Visai prie pat stačiatikių, liuteronų ir katalikų bažnyčių išsidėstę kaimiško tipo restoranai turistams, o tuos, kas jau pasisotino, madingi naktiniai klubai kviečia užbaigti vakarą šokiais. Estijoje vyksta mažiau viengungių vakarėlių, kur puotauja jauni girti anglai, nei kaimyninėje Latvijoje, bet ir čia galima rasti ne itin padorių vietų. Vienas iš klubų yra jausmus žadinantis „Depeche Mode" baras, kuriame grojami tik baro pavadinime įamžintos devintojo dešimtmečio grupės iš Esekso įrašai ir kuris išpuoštas tarsi kultūrinio palikimo šventovė iš Margaret Thatcher ankstyvojo valdymo laikotarpio.

Neįprasta, bet maloni Talino atmosfera man pasirodė dar ryškesnė, mat atvykau savaitę prieš Jonines ir prieš pat prasidedant pasakiškoms baltosioms naktims. Sutemsta tik šiek tiek po vidurnakčio, o po pusantros valandos vėl ima aušti. Po savaitės bus šviesu kiaurą parą.

Tas imperinių ambicijų susikirtimo kratinys, savitos modernios kultūros ikonos ir fantastiška natūrali šviesa yra idealus fonas kasmetiniam Kooperacinio kibernetinės gynybos meistriškumo centro susirinkimui. Tai NATO remiamas kompleksas, tiriantis visus kibernetinių karų aspektus. Konferencijos dalyviai gyvena šiuolaikinėje stebuklų šalyje, kurioje dažnai nepaisoma formalumų – veikėjai su surištais į uodegą plaukais ir su akiniais vieliniais rėmeliais ir kariškiai krakmolytomis uniformomis rimtais veidais keičiasi informacija apie „silpnąsias struktūrizuotos užklausų kalbos SQL* įdiegimo puses". Kostiumuoti valstybės tarnautojai, įsitraukę į dalykišką pokalbį su jaunuoliais, dėvinčiais džinsus ir marškinėlius, gvildena blogį, kurį patiria atakų centre atsidūręs žmogus.

Tas, kas nori suvokti esminius daugybę aspektų turinčio kibernetinio saugumo pagrindus, turi būti pasiruošęs išmokti nesuskaičiuojamą galybę naujų terminų, kurie nuolatos atsiranda arba yra keičiami. Antraip klausysitės pokalbio, kurio pagrindinis žodynas ir sintaksės struktūra neabejotinai angliški, tačiau tiems, kas neišmano šios paslaptingos kalbos, yra visai nesuprantami. Be abejo, nesmagu visą laiką klausinėti gerai šią kalbą įvaldžiusių žmonių, kodėl, tarkim, „buferio perkrova" gali turėti nerimą keliančių pasekmių jūsų tinklo saugumui, tačiau kompiuterių fanatikai nepriklauso iš aukšto į kitus žiūrinčiųjų klanui ir paprastai džiaugiasi, galėdami padaryti paslaugą.

Nors Estija ir maža, ji yra labiausiai telefonizuota ir kompiuterizuota šalis Europoje ir viena iš pirmaujančių pasaulyje savo skaitmeniniais pajėgumais. Čia – be kitų išradimų – atsirado „Skype" programa. Nemokamas belaidis ryšys prieinamas daugelyje vietų, kadangi ryšio galimybė laikoma esmine teise, o ne privilegija. Čia

* SQL (angl. *Structured Query Language*) – populiariausia iš šiuo metu vartojamų kalbų, skirtų duomenims aprašyti ir manipuliuoti jais reliacinių duomenų bazių valdymo sistemose.

nerasite viešbučių, kur norint pasinaudoti internetu reikėtų pakratyti piniginę.

Tačiau su Hillariu Aarelaidu aš kalbėjausi ne apie pažangų Estijos požiūrį, bet apie jos gerai žinomą vietą dabartiniu metu sparčiai besirutuliuojančioje tarptautinės konkurencinės skaitmeninės technikos istorijoje.

2007 m. pradžioje Estijos vyriausybė paskelbė apie savo ketinimą perkelti memorialą Raudonosios armijos kariams, kritusiems Antrajame pasauliniame kare (rusų vadinamame Didžiuoju tėvynės karu), iš jo buvusios vietos pačioje Talino širdyje į pagrindines miesto kapines, kurios, tiesą sakant, yra netoli nuo miesto centro. Rusija ir jos vadovybė suvokė tai kaip nepakeliamą įžeidimą, net kaip fašistinio Estijos nacionalizmo atgimimą ir paniekinimą tų Raudonosios armijos karių, kurie paaukojo gyvybę, vaduodami Estiją iš nacių jungo.

Ginčai dėl bronzinio kareivio virte virė. Rusijos žiniasklaida tiek pačioje Estijoje, tiek ir kaimyninėje Rusijoje kurstė tikrą Estijoje gyvenančių rusų mažumos nerimą, ir netrukus ši problema pasiekė lūžio tašką. Birželio 27 d. popietę šimtai jaunų rusų, atstovaujančių Estijos gyventojų tautinei mažumai, susirinko Talino centre. Protesto demonstracija prieš memorialo perkėlimą vyko taikiai ir geranoriškai tol, kol viena grupė pabandė prasilaužti pro skulptūrą saugantį policijos kordoną. Greitai kilo ir plito įnirtingi susidūrimai – vakare senamiestis, UNESCO paveldo objektas, jau liepsnojo, nes buvo padeginėjami automobiliai, daužomi langai ir plėšiamos už jų esančios patalpos.

Kilus grėsmei, kad neramumai plis, Maskva paskelbė įspėjimą, pabrėždama Estijos policijos brutalumą. Šalį, mažiau nei prieš du dešimtmečius atgavusią nepriklausomybę nuo Sovietų Sąjungos, apėmė netikrumas ir baimė. Neatrodė, kad Rusija siūlytų Estijai „brolišką paramą“ (taip rusai buvo pavadinę savo tankų įsiveržimą).

Pagaliau juk dabar Estija buvo NATO narė ir atrodė neįtikėtina, kad dėl sukruvintos statulos Rusija panorėtų suteikti dingstį NATO imtis įgyvendinti saugumo garantijas pagal principą „vienas už visus, visi už vieną".

Visų mūsų laimei, Kremlius iš tiesų neparodė noro suteikti kokią nors brolišką paramą, bet tuo metu, kai Talino centras pyškėjo ir gaudė nuo riaušininkų ir vėliavų degintojų, programišiai atidarė naują šio ypatingo konflikto frontą.

Tą vakarą Estijos prezidento ir kelių ministerijų interneto svetaines užplūdo daugybė brukalo, o ministro pirmininko nuotrauka buvo išmesta iš jo partijos interneto svetainės. Rusakalbių pokalbių svetainės ragino programišius atakuoti Estijos svetaines ir platino programinę įrangą, leidžiančią tai padaryti. Remiantis šaltiniais, cituojančiais Jungtinių Valstijų ambasados telegramą į Vašingtoną (pagal „WikiLeaks"), pirmosios atakos buvo techniškai nesudėtingos ir „labiau priminė kibernetines riaušes nei kibernetinį karą".

Tačiau per savaitgalį elektroninio brukalo liūtis peraugo į DDoS atakas. Programišiai sukūrė gausybę tų baisių kenkėjiškomis programomis užkrėstų kompiuterių tinklų, užvaldančių užkrėstus kompiuterius-zombius visame pasaulyje ir verčiančių juos kreiptis į Estijos interneto svetaines. Tai buvo galingi puolimai: anot JAV ambasados kabelinės televizijos pranešimo, prezidento svetainė, „kurios pajėgumas paprastai yra du milijonai megabitų per sekundę, buvo užversta beveik 200 milijonų megabitų per sekundę informacijos srautu". Visa tai dar buvo suvaldoma, bet gegužės 3 d. „kibernetinės atakos išplito už Estijos vyriausybinių svetainių ir serverių ribų į privačias svetaines".

Tą vakarą, apie dešimtą valandą, Jaanas Priisalu savo namuose Talino priemiestyje sulaukė skambučio. „Jie man pasakė, kad darbe visi ryšių kanalai nebeveikia", – prisiminė jis. Didžiausio Estijos

banko „Hansabank“ Informacinių technologijų saugumo skyriaus viršininkas Priisalu įsiaudrino. „Paskui gavau SMS žinutę, informuojančią, kad mūsų internetinės bankininkystės paslauga nebegalima naudotis.“

Iš visų pusių sklido įspėjimai ruoštis blogiausiam: dešimtys tūkstančių kompiuterių beldėsi į „Hansabank“ sistemas, reikalaudami informacijos. Priisalu nedelsdamas pradėjo karštligiškai veikti ir greitai išsiaiškino, kad bankas „Hansabank“ yra atakuojamas kenkėjiškomis programomis užkrėstų kompiuterių tinklo, kurį sudaro apie 80 000 kompiuterių. Bandydamas atsekti atakų šaltinį, Priisalu išsiaiškino, kad jos ateina iš Malaizijoje esančio serverio. Tai, be abejo, nieko nereiškė, nes Malaizija tebuvo tikrųjų užpuolikų priedanga. Tačiau jis iš karto suprato, kad tai labai rimtos atakos. „Jos buvo masinės“, – sakė jis. 80 000 kenkėjiškomis programomis užkrėstų kompiuterių tinklas yra milžiniškas monstras, galintis per kelias minutes visiškai paralyžiuoti visą kompanijos sistemą.

Kadangi Priisalu laiku ėmėsi prevencinių priemonių, „Hansabank“ buvo gerai pasiruošęs ir turėjo galingus serverius. Egzistavo alternatyvios svetainės, kurios buvo tarsi pagrindinių svetainių veidrodinis atspindys (todėl DDoS atakos nebuvo tokios sėkmingos, kokios galėjo būti). Tačiau nors „Hansabank“ svetainė ir išliko prieinama naudotojams, JAV ambasados pagrindinis informacinis šaltinis Estijoje pranešė, kad šios atakos kompanijai kainavo „mažiausiai 10 milijonų eurų (13,4 milijonų dolerių)“.

Kiti atakų objektai buvo Estijos žiniasklaida, įskaitant pagrindinį dienraštį kartu su dažniausiai lankoma naujienų svetaine. „Pamėginkite įsivaizduoti psichologinį poveikį, – pasakojo apžvalgininkas, – kai estai mėgino, bet negalėjo apmokėti sąskaitų arba negalėjo perskaityti žinių internete.“ Vyriausybė buvo pasirengusi pavojui, rimtai susirūpinusi, kad vis stiprėjančios atakos kelia „bauginančią grėsmę pagrindinei ekonominei ir socialinei infrastruktūrai“.

Iki to laiko Hillaris Aarelaidas ir jo komanda jau buvo visiškai mobilizuoti. Estijos reagavimo į kompiuterinio saugumo incidentus grupė ėmėsi atsakomųjų priemonių ir, padedama draugų iš užsienio, ypač iš Suomijos ir Švedijos, padidino į šalį ateinančių plačiajuosčio ryšio kanalų skaičių. „Mes tikėjomės, kad gali atsitikti kažkas panašaus, ir buvome pasirengę, – prisiminė Hillaris. – Štai čia rusai ir padarė klaidą. Norint, kad tokia kaip ši ataka pasisektų, reikia labai gerai pažinoti savo priešą ir būti netoli jo, – pasakė jis ir pabrėžė, kad rusai nenumatė aukšto Estijos pasirengimo lygio. – Jei jie būtų visa tai gerai apgalvoję, – aiškino jis, – jie būtų žinoję, kad dėl neseniai įvykusių rinkimų mūsų sistemos buvo gerai paruoštos."

Vyriausybės, policijos, bankų ir RKSIG koordinuotomis pastangomis atakų poveikis paprastiems žmonėms neperžengė priimtinų ribų. „Hansabank" internetinė bankininkystė veikė, bet analogiška kitų dviejų didžiausių bankų paslauga buvo neprieinama. Žmonės paprasčiausiai pradėjo naudotis jų filialų paslaugomis. Mobiliųjų telefonų ryšys sutriko, o kai vyriausybė įsakė nutraukti Estijos ryšius su išoriniu pasauliu, keletą dienų su šalimi buvo keblu susisiekti. Priešingai nei buvo teigiama pirmuosiuose pranešimuose, šviesoforai Taline nenustojo veikti, bet vyriausybės ir žiniasklaidos darbas iš tiesų buvo šiek tiek pakrikęs.

Įvairaus intensyvumo atakos tęsėsi dvi savaites, o jas vainikavo didžiulis puolimas gegužės devintąją, Raudonosios armijos pergalės prieš nacistus Europoje dieną. Tada negailestingų DDoS atakų antplūdžio išvarginta Estijos vyriausybė nusprendė atjungti šalies interneto sistemą nuo likusio pasaulio. DDoS atakos sumažėjo ir galiausiai gegužės 19 d. baigėsi.

Estijos įvykiai turėjo didžiulę reikšmę. Kalbant politiniais terminais, buvo visiškai aišku, kad atakos ėjo iš Rusijos, bet, kaip ir buvo galima numatyti, Maskvos vyriausybė neprisiėmė jokios atsakomybės. Ir labai tikėtina, kad jokios oficialios institucijos su jomis

nebuvo susijusios. Tyrėjai nesugebėjo atsekti tikslaus atakų šaltinio. Tačiau jei manoma, kad jos atėjo iš Rusijos, tai vyriausybė, turėdama visažinę monitoringo sistemą SORM-2, turėjo apie jas žinoti. Tai pasakius, vis dėlto reikia paminėti, kad tuo metu Rusijoje vyko tiek daug nepaprastai svarbios internetinės veiklos, jog gali būti, kad net garsiajai SORM-2 buvo sunku su viskuo susidoroti. Kas gali pasakyti? Bet vienas dalykas po Estijos atakos tapo gana aiškus: gali labai įžvalgiai spėlioti, kas išprovokuoja panašius įvykius, bet niekada niekuo negali būti tikras.

Kaip ir visos vyriausybės, Rusijos vyriausybė laikui bėgant įgavo specifinį požiūrį į internetą, jo funkcijas ir savitarpio santykius tarp valstybės ir galutinio naudotojo. Dar praeito amžiaus paskutiniame dešimtmetyje Maskva pripažino, kad politiniu ir saugumo požiūriu internetas yra toks svarbus, jog nusipelnė vienos iš ilgiausiai išsilaikiusių ir sėkmingiausiai veikiančių šalies institucijų – slaptosios policijos – rimto dėmesio. Trumpai tariant, Rusijos Federacijos federalinė saugumo tarnyba FSB (KGB įpėdinė) sukūrė galimybę kontroliuoti kiekvieną šalies įeinančios, išeinančios ir aplink esančios informacijos paketą. Šiai sistemai sugalvotas deramas grėsmingas pavadinimas SORM-2 – *Система оперативно-розыскных мероприятий*, arba Operatyvinės paieškos priemonių sistema.

SORM-2 sistema iš tiesų yra bauginanti. Jei internetu iš savo kompiuterio Vladivostoke ar Krasnodare jūs paprašytumėte kokios nors informacijos, vos tik jūsų užklausai pasiekus internetinių paslaugų teikėją, jos dublikatas paklusniai nuskrietų į FSB centrą Maskvoje, kad būtų perskaitytas, apsvarstytas, galbūt išjuoktas arba (kas žino?), FSB malonumui, panaudotas kaip įkaltis prieš jus. Ar bent jau išsaugotas.

SORM-2 sistema ne tik reikalauja, kad Rusijos internetinių paslaugų teikėjai perduotų visą veiklos internete medžiagą į FSB būstinę, bet dar labiau apsunkina visą reikalą, versdama paslaugų teikėjus

pirkti tam reikalingą įrangą (kainuojančią daugiau nei 10 000 dolerių) ir finansuoti einamąsias paslaugos išlaidas. Šios išlaidos, be abejo, yra paskirstomos klientams, ir šie galiausiai sumoka už galingą priespaudos priemonę, kurios pagrindinės aukos yra jie patys.

Taigi Rusija turi galimybę internetu sužinoti, kas ką daro, kada, kam ir galbūt netgi kodėl. Aišku, koks nors kompiuterininkas gali patylomis sugalvoti planą, kaip pergudrauti viską matančią SORM-2, užšifruoti savo duomenis ir interneto naršyklę. Bet neužmirškite – šifravimas Rusijoje laikomas nelegaliu ir vieno failo su skaitmeniniu užraktu pakaktų, kad jums būtų nupirktas vienpusis bilietas į Sibirą.

Tai nereiškia, kad Vakarų šalių vyriausybių internetiniai režimai toleruoja kalbos laisvę. Priešingai, augant mūsų internetinei nepriklausomybei, taip pat stiprėja ir vyriausybių norai, gebėjimai ir ketinimai ją kontroliuoti. Nepaisant nuolatinių valstybės tarnautojų ir politikų pareiškimų, kad toks procesas nevyksta, kankinanti ir lėta internetinio privatumo mirtis Vakaruose, ypač Jungtinėje Karalystėje ir Jungtinėse Valstijose, yra liūdna, nors akivaizdi ir galbūt neišvengiama realybė.

Kaip atsakas į Rugsėjo 11-ąją, kovojant su terorizmu, buvo smarkiai apribota mūsų teisė išvengti valstybės kišimosi į internetą. Pagrindinė priemonė Jungtinėse Valstijose – Bendro informacinio supratimo programa TIA, nors netgi iš prigimties kurčia Busho administracija galiausiai suprato, kad šis pavadinimas turi tiek daug asociacijų su anglų rašytojo ir žurnalisto Geoge'o Orwello kūryba, jog jį reikėtų pakeisti į „Informacinio supratimo apie terorizmą programa".

TIA pagimdė Pažangių gynybos tyrimų projektų agentūrą DARPA (angl. *Defense Advanced Research Projects Agency*). Tai Pentagono tyrimų ir sekimo padalinys, turintis plačią prieigą prie duomenų, surinktų iš privačių pokalbių. Nors agentūra galiausiai buvo

uždaryta, vyriausybė išsaugojo daugelį jos galimybių ir paskirstė jas tarp įvairių Jungtinių Valstijų institucijų.

Kitur Aukščiausiasis teismas, darydamas išimtinį sprendimą, pritarė FTB, siunčiančiai klaviatūros sekimo trojanus į įtariamųjų asmenų kompiuterius, su sąlyga, kad tai būtų atliekama prižiūrint teismui. Tai sudarė galimybes FTB registruoti viską, kad ir ką įtariamasis darytų savo kompiuteryje, taigi elgtis taip, kaip tai daro internetiniai nusikaltėliai, užkrėsdami trečiosios šalies kompiuterį klaviatūros sekimo programa. Pereinamuoju į naująjį tūkstantmetį laikotarpiu Europos Parlamentas patvirtino Jungtinių Valstijų globalaus šnipinėjimo programos „Echelon" egzistavimą, kaip teigiama, ji gali sekti skaitmenines komunikacijas bet kuriame pasaulio kampelyje.

Direktyvoje, kuri buvo išleista, kai Europos Sąjungai pirmininkavo Didžioji Britanija, Europos internetinių paslaugų teikėjai buvo įpareigoti pradėti kaupti visus kompiuteriais perduodamus duomenis (tas pats yra taikoma ir mobiliesiems telefonams) ir saugoti juos nuo šešių mėnesių iki dvejų metų – tai duomenys, prie kurių, remiantis nacionaliniais įstatymais, gali prieiti įvairios vyriausybinės institucijos. Jei tokie veiksmai, palaikantys skaitmeninę priežiūrą ir sekimą, tęsis, Vakarų vyriausybės (paprastai prisidengdamos antiteroristinėmis strategijomis ir teisėsauga) vis lengviau galės sekti savo piliečių elgesį ir įpročius.

Londono ekonomikos mokyklos tyrėjai geriausiai apibūdino mūsų pasirinktą kelią. 2009 m. birželį jie paprašė skaitytojų įsivaizduoti:

> vyriausybę, turinčią kurčią saugumo agentą, sekantį kiekvieną žmogų visur, kad ir kur jis būtų. Agentas nesupranta jokių pokalbių turinio, bet šiaip gali detaliai stebėti kieno nors gyvenimą: kada žmogus keliasi, kaip vyksta į darbą,

su kuo ir kiek ilgai kalbasi, kaip jam sekasi verslas, kokia jo sveikata, su kuo jis susitinka gatvėje, ar dalyvauja visuomeninėje veikloje ir kokioje, kokie jo politiniai įsitikinimai, kokius laikraščius jis skaito ir kokiais straipsniais ypač domisi, kaip į juos reaguoja, kokį maistą dedasi į pirkinių krepšį, ar sveikai maitinasi, ar sėkmingas jo santuokinis gyvenimas, ar turi nesantuokinių ryšių, o jei taip, tai su kuo susitikinėja ir turi intymių santykių. Kadangi dauguma tokių ryšių šiais laikais dažnai palaikomi per telekomunikacines ryšių priemones arba naudojantis mobiliaisias telefonais, visa ši informacija patikimai saugoma mūsų internetinių paslaugų teikėjų, paruošta taip, kad vyriausybė galėtų prieiti, ir tik ir laukianti šito.

Bent jau Vakaruose mes labai priešinamės įvairių vyriausybinių institucijų siekiui įgyti dar drakoniškesnių galių, leidžiančių kontroliuoti piliečių veiksmus internete.

Atsižvelgiant į laisvos piliečių bendruomenės stiprybę Vakaruose ir visa apimančią KGB interneto priežiūrą, būtų galima daryti prielaidą, kad Rusija yra sukūrusi itin priešišką aplinką internetiniams nusikaltėliams. Vis dėlto Rusijos Federacija tapo vienu iš didžiausių globalinių nusikaltimų centru. Policijos atakų dažnis yra apgailėtinas, o nuteistųjų skaičius retai būna dviženklis. Priežastis visiškai suprantama, nors apie ją garsiai nekalbama. Internetiniai nusikaltėliai iš Rusijos gali laisvai klonuoti tiek kreditinių kortelių, įsilaužti į tiek banko sąskaitų ir išplatinti tiek elektroninio pašto brukalo, kiek tik nori, svarbu, kad jų atakų objektai būtų iš Vakarų Europos ir Jungtinių Valstijų. Rusijos programišius, kuris imtų vogti iš rusų, dar nespėjęs ištarti KGB vardo, būtų įgrūstas į automobilį be numerių.

Be abejo, jei Rusijos valstybės pareigūnai mainais paprašytų programišiaus paslaugų, norėdami pradėti paralyžiuojančią interne-

tinę ataką prieš pastebėtą priešą, tai jam greičiausiai vertėtų sutikti bendradarbiauti.

2007 m. buvo savanoriškai susibūrusių kompanijų organizacijos, įsikūrusios Sankt Peterburge ir vadinamos Rusijos verslo tinklu, arba RBN (angl. *Russian Business Network*), klestėjimo metai. Šiuo paslaptingu trumpiniu prisidengusi organizacija siūlė prieglobą (angl. *hosting*) individualioms ir kompanijų svetainėms – ji buvo žinoma kaip neįveikiamų prieglobos serverių karalienė. Kompanijos, siūlančios šios rūšies paslaugas, paprastai būtinai informuoja savo klientus, kad nesidomės svetainių turiniu ar jų funkcijomis, o už daug didesnį mokestį priešinsis bet kokioms pastangoms teisinėmis ar skaitmeninėmis priemonėmis sužlugdyti svetaines.

Neįveikiama priegloba ne visada siekia apeiti įstatymus, bet nusikaltėliai ir piratai dažnai naudojasi tokiomis paslaugomis. Ji iš esmės yra nepakeičiama individams ir grupėms, užsiimantiems, pavyzdžiui, vaikų pornografijos platinimu, o kaip nustatė kelių saugumo kompanijų tyrėjų departamentai, Rusijos verslo tinklas turėjo būtent tokių klientų.

Šie serveriai taip pat pasirodė nepamainomi žmonėms, platinantiems elektroninį brukalą, nes tokiems operatoriams reikia didelių ir saugių pajėgumų, kad galėtų išsiuntinėti milijardus įtartinų reklamų ir virusų. Neįveikiami serveriai perša mums Nigerijos 419 apgaulę*, padirbtus vaistus, garsiąsias penio pailginimo priemones ir daug kitų produktų (tikrų ar pramanytų). Daugelis brukamų elektroninių žinučių slepia virusus arba nuorodas į virusais užkrėstas svetaines, kurios, jei yra aktyvuojamos, gali paversti kompiuterį kenkėjiškomis programomis užkrėstų kompiuterių armijos pėstininku.

* Dar vadinama Nigerijos laišku, 419 apgaule, Nigerijos suktybe, Nigerijos banko suktybe. Tai pasitikėjimu paremtas triukas, kai gavėjas įtikinamas pervesti tam tikras sumas pinigų, pažadėjus, kad paskui jis gaus gerokai didesnę sumą.

2006 ir 2007 m., klestint Rusijos verslo tinklui, per Jungtinėje Karalystėje, Kardifo mieste, vykdomą slaptą operaciją, nukreiptą prieš elektroninį brukalą, buvo išvardyti 2 048 šio tinklo kontroliuojami interneto adresai. Tada RBN buvo apibūdintas kaip „vienas iš baisiausių brukalo platintojų pasaulyje" ir plataus masto „vaikų pornografijos, kenkėjiškų programų, sukčiautojų su kreditinėmis kortelėmis ir internetinius nusikaltėlius globojančių tinklų" prieglauda.

Rusijos verslo tinklas visų pirma yra svarbus dėl pelningų ir neįveikiamų prieglobos organizacijų, kurios gali imti 600 dolerių ir dar didesnį mėnesinį mokestį. Legalių svetainių kaina sudaro dešimtąją šios sumos dalį.

Tačiau antraeilis RBN vaidmuo daugeliu atžvilgių yra dar įdomesnis. Atakos prieš Estiją prasidėjo milijonais brukamų elektroninių žinučių, kurios užgriuvo Estijos vyriausybinius kompiuterių tinklus. Vėliau François Paget, dirbantis JAV kompiuterių saugumo gigante „McAfee", išanalizavo elektroninio brukalo turinį ir nustatė, kad šios žinutės buvo visai tokios pat kaip ir standartinės RBN siunčiamos žinutės. Dar daugiau, Didžiosios Britanijos sunkių organizuotų nusikaltimų agentūros Kibernetinės žvalgybos viršininkas Andy Auldas pranešė, kad, trumpai stebėjusi RBN situaciją Sankt Peterburge, Britanijos policija sugebėjo nustatyti, jog RBN iš dalies galėjo vykdyti savo veiklą dėl to, kad papirko vietines teisėsaugos institucijas ir teismus.

Gali būti, kad Estijos atakas išprovokavo Rusijos verslo tinklas, bet tai nelabai tikėtina. Greičiausiai kažkas sumokėjo už jų paleidimą arba valdžia pasitikėjo RBN, norėdama dalyvauti šiame patriotizmo akte. Šis ryšys tarp Sankt Peterburge įsikūrusių interneto paslaugų teikėjų, kurių specializacija yra kriminalinė veikla, ir kibernetinių Estijos atakų išryškina vieną iš didžiausių kompiuterinių nusikaltimų ir kompiuterių saugumo mįslių.

Internete egzistuoja trys pagrindinės „grėsmės", kurių kiekviena pasireiškia įvairiais pavidalais. Visų pirma yra internetiniai nusikaltimai.

Pati svarbiausia jų pasireiškimo forma yra kardingas – kreditinių kortelių duomenų vogimas ir klonavimas, siekiant finansinės naudos. Be kardingo, dar yra įvairių kitų sukčiavimo būdų. Pavyzdžiui, itin pelninga yra vadinamoji gąsdinamoji programinė įranga (angl. *scareware*), kuri buvo ištobulinta Ukrainoje įsikūrusioje kompanijoje pavadinimu „Innovative Marketing"*(IM). Ši kompanija įdarbino begalę jaunų žmonių Ukrainos sostinėje Kijeve, ir dauguma jų tikėjo dirbantys naujai įsteigtoje kompanijoje, parduodančioje legalius apsaugos produktus. Tačiau tai buvo netiesa.

Kompanija siuntinėjo apgaulingą reklaminę programinę įrangą, kurią įdiegus individualaus naudojimo kompiuteryje, interneto naršyklėje iškyla langas, perspėjantis naudotoją, kad jo kompiuteris atsidūrė pavojuje, nes jį užkrėtė virusas. Reklama paaiškina, kad vienintelis būdas apsaugoti kompiuterį nuo elektroninių padarų, šliaužiojančių aplink jo standųjį diską ir operatyviąją atmintį, yra spragtelėti ant nuorodos ir nusipirkti „Kenkėjiškų programų naikiklį 2009" – vieną iš nesuskaičiuojamos galybės jų produktų.

Kai tik parsisiųsite „Kenkėjiškų programų naikiklį", IM jums nurodys pašalinti jūsų turimą antivirusinę sistemą, pavyzdžiui, „Norton", ir įdiegti jų produktą. Įdiegus jis visiškai nieko nepadaro – tai neveikli programa, tačiau dabar jūsų kompiuteris, be abejo, tampa atviras bet kurio į jį patenkančio viruso užkratui, be to, jūs už šią abejotiną paslaugą jau esate sumokėjęs.

Dirkas Kolbergas, „McAfee" kompanijos tyrėjas iš Hamburgo, pradėjo stebėti šią operaciją. Jis atsekė gąsdinamosios programinės įrangos šaltinį Rytų Azijoje ir išsiaiškino, kad IM serverių administratorius kai kuriuos prievadus buvo palikęs plačiai atvertus, taigi Kolbergas laisvai galėjo „bastytis" po serverį ir tyrinėti jį kada tik panorėjęs. Tai, ką jis atskleidė, gniaužė kvapą. Kompanija „Innovative

* Novatoriška rinkodara. (Angl.)

2006 ir 2007 m., klestint Rusijos verslo tinklui, per Jungtinėje Karalystėje, Kardifo mieste, vykdomą slaptą operaciją, nukreiptą prieš elektroninį brukalą, buvo išvardyti 2 048 šio tinklo kontroliuojami interneto adresai. Tada RBN buvo apibūdintas kaip „vienas iš baisiausių brukalo platintojų pasaulyje" ir plataus masto „vaikų pornografijos, kenkėjiškų programų, sukčiautojų su kreditinėmis kortelėmis ir internetinius nusikaltėlius globojančių tinklų" prieglauda.

Rusijos verslo tinklas visų pirma yra svarbus dėl pelningų ir neįveikiamų prieglobos organizacijų, kurios gali imti 600 dolerių ir dar didesnį mėnesinį mokestį. Legalių svetainių kaina sudaro dešimtąją šios sumos dalį.

Tačiau antraeilis RBN vaidmuo daugeliu atžvilgių yra dar įdomesnis. Atakos prieš Estiją prasidėjo milijonais brukamų elektroninių žinučių, kurios užgriuvo Estijos vyriausybinius kompiuterių tinklus. Vėliau François Paget, dirbantis JAV kompiuterių saugumo gigante „McAfee", išanalizavo elektroninio brukalo turinį ir nustatė, kad šios žinutės buvo visai tokios pat kaip ir standartinės RBN siunčiamos žinutės. Dar daugiau, Didžiosios Britanijos sunkių organizuotų nusikaltimų agentūros Kibernetinės žvalgybos viršininkas Andy Auldas pranešė, kad, trumpai stebėjusi RBN situaciją Sankt Peterburge, Britanijos policija sugebėjo nustatyti, jog RBN iš dalies galėjo vykdyti savo veiklą dėl to, kad papirko vietines teisėsaugos institucijas ir teismus.

Gali būti, kad Estijos atakas išprovokavo Rusijos verslo tinklas, bet tai nelabai tikėtina. Greičiausiai kažkas sumokėjo už jų paleidimą arba valdžia pasitikėjo RBN, norėdama dalyvauti šiame patriotizmo akte. Šis ryšys tarp Sankt Peterburge įsikūrusių interneto paslaugų teikėjų, kurių specializacija yra kriminalinė veikla, ir kibernetinių Estijos atakų išryškina vieną iš didžiausių kompiuterinių nusikaltimų ir kompiuterių saugumo mįslių.

Internete egzistuoja trys pagrindinės „grėsmės", kurių kiekviena pasireiškia įvairiais pavidalais. Visų pirma yra internetiniai nusikaltimai.

Pati svarbiausia jų pasireiškimo forma yra kardingas – kreditinių kortelių duomenų vogimas ir klonavimas, siekiant finansinės naudos. Be kardingo, dar yra įvairių kitų sukčiavimo būdų. Pavyzdžiui, itin pelninga yra vadinamoji gąsdinamoji programinė įranga (angl. *scareware*), kuri buvo ištobulinta Ukrainoje įsikūrusioje kompanijoje pavadinimu „Innovative Marketing"*(IM). Ši kompanija įdarbino begalę jaunų žmonių Ukrainos sostinėje Kijeve, ir dauguma jų tikėjo dirbantys naujai įsteigtoje kompanijoje, parduodančioje legalius apsaugos produktus. Tačiau tai buvo netiesa.

Kompanija siuntinėjo apgaulingą reklaminę programinę įrangą, kurią įdiegus individualaus naudojimo kompiuteryje, interneto naršyklėje iškyla langas, perspėjantis naudotoją, kad jo kompiuteris atsidūrė pavojuje, nes jį užkrėtė virusas. Reklama paaiškina, kad vienintelis būdas apsaugoti kompiuterį nuo elektroninių padarų, šliaužiojančių aplink jo standųjį diską ir operatyviąją atmintį, yra spragtelėti ant nuorodos ir nusipirkti „Kenkėjiškų programų naikiklį 2009" – vieną iš nesuskaičiuojamos galybės jų produktų.

Kai tik parsisiųsite „Kenkėjiškų programų naikiklį", IM jums nurodys pašalinti jūsų turimą antivirusinę sistemą, pavyzdžiui, „Norton", ir įdiegti jų produktą. Įdiegus jis visiškai nieko nepadaro – tai neveikli programa, tačiau dabar jūsų kompiuteris, be abejo, tampa atviras bet kurio į jį patenkančio viruso užkratui, be to, jūs už šią abejotiną paslaugą jau esate sumokėjęs.

Dirkas Kolbergas, „McAfee" kompanijos tyrėjas iš Hamburgo, pradėjo stebėti šią operaciją. Jis atsekė gąsdinamosios programinės įrangos šaltinį Rytų Azijoje ir išsiaiškino, kad IM serverių administratorius kai kuriuos prievadus buvo palikęs plačiai atvertus, taigi Kolbergas laisvai galėjo „bastytis" po serverį ir tyrinėti jį kada tik panorėjęs. Tai, ką jis atskleidė, gniaužė kvapą. Kompanija „Innovative

* Novatoriška rinkodara. (Angl.)

Marketing“ uždirbdavo tiek pinigų, kad įsteigė tris skambučių centrus – vieną kalbantiesiems angliškai, antrą kalbantiesiems vokiškai, trečią kalbantiesiems prancūziškai; šie centrai sutrikusiems klientams turėjo padėti įdiegti nefunkcionuojančius kompanijos produktus.

Iš pajamų dokumentų, kuriuos taip pat rado serveryje, Kolbergas suprato, kad apgavystės, naudojant gąsdinamąją programinę įrangą, administracijai uždirbo dešimtis milijonų dolerių, ir tai buvo vienas iš teatrališkiausių internetinių nusikaltimų pavyzdžių.

Be gąsdinamosios programinės įrangos, yra sukčiavimo su akcijomis ir vertybiniais popieriais metodas (angl. *pump-and-dump*): programišiai įeina į finansines svetaines ir skaitmeniniu būdu smarkiai pakelia akcijų vertę, tada parduoda savo turimas akcijas, o paskui vėl numuša akcijų vertę internete. Taip pat yra „algalapių schemos“: nusikaltėliai įsilaužia į stambių korporacijų kompiuterius ir į personalo duomenų bazę įrašo neegzistuojančius darbuotojus. Tačiau programišiai šiems darbuotojams priskaičiuoja realius atlyginimus, kurie kas mėnesį išsiunčiami vadinamiesiems „pinigų mulams“. Jiems nurodoma už nedidelį atlygį pervesti pinigus į banką, esantį tolimoje šalyje, iš kurios iš tiesų ir buvo vykdomas nusikaltimas.

Internetas siūlo beribes galimybes kūrybiškiems protams teisiniame pasaulyje, bet lygiai taip ir nusikaltėliai internete gali duoti valią savo fantazijai.

Antra svarbi internetinių piktadarybių sritis yra kibernetinis pramoninis šnipinėjimas. Remiantis kasmetine grėsmių ataskaita, kurią paskelbė Amerikos telekomunikacijų milžinė „Verizon“, ši sritis apytikriai sudaro 34 procentus nusikalstamos veiklos internete ir beveik neabejotinai yra pati pelningiausia. Ryšių technologijos leidžia vogti pramonines paslaptis daug lengviau nei kitados. Kol kompiuteriai nebuvo taip plačiai paplitę, norint ką pavogti, reikėjo fiziškai įsibrauti į kompaniją arba, jei tai buvo daroma iš vidaus, rasti būdų, kaip realiai panaikinti ar paskirstyti reikiamus duomenis.

Dabar tokių problemų nebeliko: pramoniniai vagys gali įsilaužti į korporacijų sistemas ir iššniukštinėti jų projektus, rinkodaros strategijas, algalapius ar bet kurią kitą dominančią medžiagą, o paskui visa tai parsisiųsti. Dar tada, kai Maksas Vizija nebuvo tapęs garsiuoju Ledo Žmogumi, jis dirbo „prasiskverbimo tyrinėtoju" visoje Vakarų pakrantėje – kompanijos jam mokėjo už skaitmeninio įsilaužimo bandymus. Vizija, vilkintis kalėjimo uniformą – oranžinį kombinezono tipo kostiumą, kalbėdamas su manimi pasakė: „Tais laikais buvo tik viena kompanija, į kurią man nepasisekė įsibrauti. Tai stambi Amerikos farmacijos kompanija." Ir tai suprantama – farmacinių kompanijų vertę sudaro jų moksliniai tyrimai, o praradus naujų vaistų formules galima netekti šimtų milijonų dolerių ir gali kristi akcijų vertė.

Vizija buvo smarkiai įniršęs, kad nesugebėjo įsilaužti į šią vienintelę sistemą. „Tada aš, be abejo, pradėjau suktą ataką ir po penkių minučių jau buvau sistemos viduje, bet tai ne tas pats." Kalbėdamas apie ataką, jis norėjo pasakyti, jog kompanijos adresais jis pasiuntė užkrėstų elektroninių žinučių ir vos po kelių minučių vienas iš daugelio tūkstančių kompanijos darbuotojų įkliuvo į spąstus. Taigi, net susidūrus su nepralaužiama skaitmenine tvirtove, reikia įveikti tik vieną iš kelių svarbiausių saugumo iššūkių.

Be to, šiais laikais daug lengviau atlikti šį darbą iš vidaus, nes rinkti ir kaupti kompanijų duomenis nėra sunku. Žinome, kad Bradley Manningas, žmogus, apkaltintas nutekinęs JAV diplomatinių misijų konfidencialią informaciją, vėliau paskelbtą „WikiLeaks" interneto svetainėje, sugebėjo perkelti visą medžiagą į kompaktinį diską, pavadintą Lady Gagos albumu.

Mes taip pat žinome, kad „Stuxnet" – pats sudėtingiausias iš iki šiol sukurtų virusų – greičiausiai buvo kažkieno infiltruotas (sąmoningai ar ne) į konkretų taikinį Irano branduoliniuose įrenginiuose per atmintuką ar kompaktinį diską ir taip užkrėtė

kompiuterių sistemas. Irano branduolinės operacinės sistemos nesinaudoja interneto ryšiu. Tačiau jos vis vien yra kompiuterių tinklai, o jų užkrėtimas „Stuxnet" virusu įrodo, kad jos buvo prieinamos profesionaliai žvalgybos agentūrai.

„Stuxnet" virusas byloja apie trečios pagal svarbą grėsmės – kibernetinio karo – eskalaciją. Ši kenkėjiška programa yra tokia sudėtinga, kad tyrėjai apskaičiavo, jog jai sukurti tikriausiai reikėjo kelerių darbo metų, vadinasi, atsidavusių programuotojų inžinierių komanda prie jos turėjo dirbti ilgą laiką. Organizuotų nusikaltėlių grupės taip nedirba. Vienintelis subjektas, galėjęs sukurti „Stuxnet", yra valstybė, turinti gausybę išteklių, kuriuos gali skirti tiek gynybinių, tiek puolamųjų kibernetinių ginklų projektavimui ir gamybai. Šiaip ar taip, tie, kas kūrė „Stuxnet", daugybę kompiuterinių programų ir programavimo metodų pasiskolino iš dešimčių tūkstančių internetinėje erdvėje veikiančių programišių, žargonu vadinamų juodkepuriais ar pilkakepuriais. Nusikaltėliai programišiai yra didelė ir kūrybinga jėga visose tamsiosios interneto pusės srityse. Kariškiai, privatūs asmenys, policija ir žvalgybos institucijos visada greitai pritaiko programišių ir įsilaužėlių sukurtas priemones.

Kai „Stuxnet" virusas buvo sėkmingai infiltruotas į kelių Irano branduolinių įrenginių kontrolės sistemas, valdžios institucijos pripažino, jog tai sukėlė rimtų labai jautrios stoties gedimų. Viskas galėjo baigtis net sprogimu. Viruso egzistavimas įrodo, kad vadinamųjų kibernetinio karo karių pateikiami pasaulio pabaigos scenarijai jau nebėra tik teorija. Estijos ataką, kuri tuo metu atrodė labai rimta, galima prilyginti žaismingai iš anksto suderintai treniruotei, palyginti su tuo, ką pranašauja „Stuxnet".

Kibernetinio karo kariai, dar vadinami kibernetinio saugumo fanatikais, – tai pranašai, kurie mus įspėja, kad dangus gali užkristi mums ant galvos. Vienas iš iškalbingiausių šios padermės atstovų

yra Richardas Clarke'as, kuris savo knygoje *Kibernetinis karas* (*Cyber War*) aprašo tokį scenarijų:

> Įėjęs į Situacijų kambarį, jūs sužinote, kad Gynybos informacinės sistemos tarnybos direktorius jau laukia jūsų, norėdamas pasikalbėti saugiu telefonu.
>
> Federalinė nepaprastųjų situacijų valdymo agentūra FEMA pranešė apie gaisrus ir sprogimus didelėse naftos perdirbimo gamyklose Filadelfijoje ir Hjustone, taip pat apie mirtinai pavojingus chloro dujų debesis, pasklidusius iš kelių chemijos gamyklų Naujajame Džersyje ir Delavere.
>
> Nacionalinis oro eismo valdymo centras Herndone, Virdžinijos valstijoje, patyrė visišką sistemų griūtį...

Dauguma saugumo fanatikų įrodinėja, jog vienintelis būdas išvengti skaitmeninio Perl Harboro ar Kibergedono yra investuoti lėšas į specialistų ir mokslininkų kolektyvus ir kompanijas, siekiant paspartinti grėsmių tyrimą.

Tai jau iš tiesų vyksta. Estijos įvykiai pagreitino judėjimą kibernetinės erdvės sukarinimo link. 2005 m. NATO pirmoji sutiko įkurti skambiai pavadintą Kooperacinį kibernetinės gynybos meistriškumo centrą Taline. Nors operacijų, skirtų kovai su kibernetiniais karais, instituto idėja buvo entuziastingai sutikta, šalys narės neskubėjo kloti pinigų ant stalo (išskyrus, suprantama, Estiją – šalį šeimininkę). Projektas nebuvo atidėtas ilgam, bet pažengė ne ką toliau nei patrauklaus dizaino firminio popieriaus užrašams sukūrimas.

„Tačiau vos prasidėjus atakai, – teigia žymus Estijos matematikas ir vienas iš centro įkūrėjų Peeteris Lorentsas, – atmosfera pasikeitė ir mes pradėjome gauti realią paramą tiek iš Briuselio, tiek iš

Vašingtono. Iš tiesų, išgirdus apie ataką, mano pirmoji reakcija buvo paskambinti į Prancūziją, užsakyti dvi dėžes prabangiausio „Cristal" šampano ir pristatyti jas ponui Putinui. Pradėdami šią ataką, rusai iš tiesų garantavo ateitį mūsų centrui."

Vašingtone, be abejo, suskambo pavojaus varpai. Įvykiai, vienas po kito nutikę prieš pat Estijos incidentą ar tuoj po jo, 2009 m. įtikino naująją Obamos vyriausybę, kad kibernetinis saugumas turi būti sustiprintas bet kokia kaina. Ypač kai praėjus keliems mėnesiams po Estijos įvykių milžiniška Amerikos sekimo organizacija – Nacionalinio saugumo agentūra (NSA) ėmė suprasti, kiek daug laimėjo Kinijos oro pajėgos, 2001 m. balandį amerikiečiams praradus žvalgybinį lėktuvą EP-3E ARIES. Tiesa, prieš lėktuvui nusileidžiant avariniu būdu, lakūnui pavyko sunaikinti programinę įrangą, tačiau techninė įranga liko nesugadinta, ir kai tik ji pateko kinams į rankas, jie pradėjo analizuoti modernias technologijas, leidžiančias patikrinti ir iššifruoti užkoduotą bendravimą. Kai po rinkimų Obama pateko į Baltuosius rūmus, netrukus kinai pradėjo savo naujo žaisliuko bandymus, o Nacionalinio saugumo agentūra atkreipė dėmesį į jų naujus sugebėjimus perimti informaciją. Atrodo, kad Vašingtonui kinai norėjo pademonstruoti, jog jiems pavyko sėkmingai įsilaužti į amerikiečių technologijas.

Jungtinių Valstijų vyriausybė nenustojo daryti įtakos Kibernetinės gynybos centrui Taline, kuris nuo 2008 m. vykdo svarbius tyrimus, tarp jų ir kompleksines kibernetines karines pratybas. Tiek Gynybos skyriaus infrastruktūrai, tiek šio skyriaus puolamųjų ir gynybinių veiksmų pajėgumams kompiuterių tinklai buvo tapę tokie svarbūs, kad Gynybos skyriaus sekretorius Robertas Gatesas padarė reikšmingą sprendimą įkurti naują karinį domeną – kibernetinę erdvę.

Ši penkta karinė teritorija, gimininga žemės, jūros, oro ir kosmoso erdvėms, yra pati pirmoji žmogaus sukurta karinių operacijų erdvė, nors joje galiojančios kovos taisyklės beveik nesuprantamos.

Kartu su domenu Pentagonas įsteigė JAV kibernetinę komandą US-CYBERCOMMAND priešiškiems veiksmams internetinėje erdvėje kontroliuoti ir, reikalui esant, puolamųjų ginklų, panašių į „Stuxnet" virusą, dislokavimui planuoti. Šiuo metu JAV yra pripažinta lyderė pagal kibernetinius puolamuosius pajėgumus.

Kibernetinių puolamųjų pajėgumų nereikėtų painioti su galimybe dislokuoti įprastinius ginklus, kurie aprūpinti kompiuterinėmis sistemomis. Geriausi pastarojo arsenalo pavyzdžiai yra radijo bangomis valdomi lėktuvai (JAV juos nuolatos dislokuodavo Afganistane ir Pakistane), kurie gali vykdyti stebėjimo ir kovines misijas, valdomi kompiuterių operatoriaus, esančio Nevadoje.

Kibernetiniai ginklai – tai įsilaužimo priemonės, kurios leidžia kibernetiniam kariui prasiskverbti į priešo ypatingos svarbos nacionalinės infrastruktūros kompiuterines sistemas, pavyzdžiui, valdančias priešo energetinius ir vandens tiekimo tinklus. Pagal karinę doktriną, galėdamas valdyti sistemą, kibernetinis vadas gali duoti nurodymą ją išjungti (arba, kaip žinome iš „Stuxnet" viruso atvejo, sukelti sprogimą, kuris padarytų didžiulę žalą), taigi per kelias dienas puolimo paveiktai visuomenei tektų grįžti prie akmens amžiaus technologijų.

Bent jau tokia yra idėja. Dabartiniu metu pripažįstama, kad Jungtinės Valstijos pirmauja kuriant puolamuosius kibernetinius ginklus. Tačiau kinai, prancūzai ir izraeliečiai lipa joms ant kulnų, o nuo jų ne ką atsilieka indai ir britai.

Kibernetinės erdvės militarizavimą buvo galima numatyti. Tačiau niekas nesupranta, kur visa tai mus nuves. Žurnalui *The New Yorker* rašantis įžvalgusis Seymouras Hershas pasišaipė iš padarytų prielaidų, kad kinai įspėjo paslaptis, įrašytas žvalgybinio lėktuvo standžiajame diske:

> Lėktuvo EP-3E kritimas sukėlė ilgalaikius debatus tarp kariškių ir Obamos administracijos atstovų. Daugelis karinių

> lyderių kinų prasiskverbimą vertino kaip perspėjimą dėl pažeidžiamumo dabar ir ateityje – kaip Kinijos ar kokios nors kitos šalies galimybę panaudoti savo tobulėjančius kibernetinius įgūdžius Amerikos civilinei infrastruktūrai ir kariniams kompleksams atakuoti. Kitoje barikadų pusėje yra tie, kurie įrodinėja, kad visuomenė turi reaguoti į grėsmę, atkreipdama dėmesį į platesnį šifravimo panaudojimą. Jie baiminasi, kad per didelis pasitikėjimas kariuomene turės neigiamų pasekmių privatumui ir piliečių laisvėms.

Regis, kariškių skubėjimas įsitvirtinti kibernetinio saugumo vyriausiųjų arbitrų pozicijose plačiai plinta. 2010 m. spalį prezidentas Obama Pentagonui priklausančią Nacionalinio saugumo agentūrą įpareigojo padėti Krašto apsaugos departamentui ir privačiam sektoriui vidaus kibernetinio saugumo klausimais. Pagrindinė Kinijos institucija, atsakinga už užsienio ir vietinį kibernetinį saugumą, yra Liaudies išlaisvinimo armija, o Artimuosiuose Rytuose ypatingųjų kompiuterinių karų tyrimų iniciatorius yra Izraelio gynybinės pajėgos, ir tai sudaro sąlygas Izraeliui pasiekti daug daugiau, nei atrodo įmanoma.

Tačiau jūs teisėtai galite paklausti, kas gi turi užsiimti visais tais su kibernetiniais nusikaltimais susijusiais reikalais?

Grėsmės kibernetinėje erdvėje yra realios ir pavojingos. Idealiu atveju demokratinė valstybė turėtų užtikrinti, kad šios svarbios technologijos duotų naudą, o ne griautų jos piliečių gyvenimą. Lygiai taip pat valstybė turėtų atsispirti pagundoms pažeisti mūsų teises ir privatumą. Visiškai neprotinga yra leisti kariškiams prisiimti vadovaujantį vaidmenį saugant civilinius tinklus. Tačiau turint omenyje, jog kibernetiniai ginklai turi tokį potencialą, kad gali pakenkti šalies ypatingos svarbos nacionalinei infrastruktūrai (ir taip sugriauti žmonių gyvenimą), kariškiai privalo būti pasiruošę

įsikišti susidarius ekstremalioms situacijoms. Tai turi būti nepaprastos aplinkybės, kurių egzistavimą galima įrodyti.

Už trijų atskirų grėsmių – internetinių nusikaltimų, kibernetinio pramoninio šnipinėjimo ir kibernetinių karų – kontroliavimą turėtų būti atsakingos atskiros institucijos. Tokios pripažintos policijos institucijos kaip FTB ar JAV slaptoji tarnyba turėtų prisiimti atsakomybę už internetinius nusikaltimus. Korporacijos ir kompanijos turėtų arba pačios susikurti savo tinklų apsaugos sistemas, arba sumokėti kompanijoms, kurios specializuojasi kibernetinės apsaugos srityje, kad jos tai padarytų. Pilietinės vyriausybės turėtų pasirūpinti savo tinklų apsauga, o kariškiai – saugoti savo sistemas.

Iš pažiūros tai atrodo gana paprasta. Tačiau realiame pasaulyje dėl interneto tarpusavio ryšių šios ribos yra sunkiai nustatomos. Antra vertus, lig šiol niekaip neišsprendžiama pagrindinė kibernetinio saugumo problema: kaip iš tiesų atrodo kibernetinė ataka?

Norėdami atsakyti į šį klausimą, kibernetinių interesų gynėjai turi išsiaiškinti du gyvybiškai svarbius dalykus. Iš kur kyla ataka? Ir – koks užpuoliko motyvas? Susidūrus su įgudusiu kibernetiniu agresoriumi, net geriausiems gynėjams nepavyksta rasti atsakymų. Lieka tik spėlioti, bet tai gali privesti prie neteisingų sprendimų, nesusipratimų ir galiausiai – konfliktų.

Tarkime, kad mūsų policijos institucijos, verslo sektorius ir kariškiai paklusniai vykdo savo užduotį saugoti valstybę nuo minėtų pavojų. Plačiame grėsmių spektre visada dalyvauja du pagrindiniai veikėjai: šnipas ir programišius. Pirmasis siekia įminti galvosūkį (bet nebūtinai pasidalija įgytomis žiniomis); antrasis, tiesą sakant, turi suformuluoti galvosūkį taip sumaniai, kad jis taptų neįmenamas.

Žvalgybos agentūros tylutėliai šniukštinėja po internetą kaip juodos katės juodame fone ir bendrauja tik tada, kai jų komandos siekia kuo nors apsimesti, ką nors užverbuoti ar supainioti. Šis šmėkliškas elgesys iš dalies užkoduotas šnipo genuose,

bet jį taip pat galima paaiškinti žvalgybos tarnybų žavėjimusi ir netgi gėrėjimusi savo pagrindiniu priešininku kibernetinėje erdvėje – programišiumi.

Dar neseniai interneto gynėjai buvo įsitikinę, kad atakas visada organizuoja programišiai. Pastaraisiais metais situacija pasikeitė, atsiradus kenkėjiškoms programoms, kurių galima nusipirkti iš „prekių atsargų". Daugelis nusikaltėlių programišių dabar užsidirba pinigų ne sukčiaudami su kreditinėmis kortelėmis, bankų sąskaitomis ar užsiimdami panašiomis suktybėmis, bet paprasčiausiai pardavinėdami savo sukurtus trojanus, virusus ir kirminus. Tai naudotojui patogios programos, kurioms panaudoti nereikia ypatingų žinių. Plačiausiai paplitusios kenkėjiškos programos, kuriomis galima užkrėsti kompiuterių tinklus. Kartais programišiai išnuomoja tokias programas dienai ar dviem, o kartais savaitei ar mėnesiui, kad jos būtų panaudotos DDoS atakoms, norint ką nors apiplėšti ar kam atkeršyti. Savaime suprantama, programišiai, kurie parduoda ar nuomoja kenkėjiškas užkrečiančias programas ar virusus, turi techninių galimybių kontroliuoti nuomos terminą, nes gali paprasčiausiai užprogramuoti jo baigimosi datą, o jų klientai – greičiausiai smulkiais atsitiktiniais darbeliais užsiimantys nusikaltėliai – nieko nepajėgs padaryti.

Vis dėlto antrinės rinkos atsiradimas, sudarantis galimybę internete nusipirkti kenkėjiškų programų, nepakeis fundamentalios tiesos, kad už bet kokios kibernetinės atakos – ar tai būtų kriminalinė internetinė ataka, ar pramoninis šnipinėjimas, ar kibernetinis karas – slypi talentingas programišius. Norint surengti kibernetines atakas, kurios ne šiaip sau sukelia nepatogumų, bet iš tiesų padaro daug žalos ir nuostolių, neabejotinai reikia aukštos specializacijos ir techninių įgūdžių. Vadinasi, net ir tuo atveju, kai programišius dirba savo viršininko (ar tai būtų mafijos bosas, ar kompanijos vadovas, ar kariuomenės vadas) naudai, norėdamas sukurti tinkamą

produktą, jis turės daug žinoti apie numatytą taikinį. Pavyzdžiui, kad ir kokia buvo programišių komanda, sukūrusi „Stuxnet“ virusą, ji turėjo ne tik išmanyti apie objektus – Irano branduolinius įrenginius, bet ir suprasti, kaip veikia juos valdantis „Siemens PLC“ tinklas ir ypatingas kompresorius, kurį suprojektavo Suomijos kompanija „Vachon“ (nors pagamintas jis buvo Kinijoje), taip pat žinoti apie Taivano kompaniją, kurios „RealTek“ skaitmeninis sertifikatas buvo padirbtas tam, kad būtų galima suklaidinti sistemos antivirusinę programą. Bet kuris, toks sumanus, kad galėtų dirbti prie „Stuxnet“ viruso, taip pat turi būti toks pat sumanus, kad perprastų savo numatytą auką.

Šiuo požiūriu programišių vaidmuo, sprendžiant kibernetinio saugumo klausimus, labai svarbus, nes jie žino problemų sprendimą. Susiraskite programišių, ir jūs būsite padaręs rimtą šuolį tiesos atskleidimo link.

Didžiulė dalis pinigų, kuriuos vyriausybės dabartiniu metu nukreipia į kibernetinį saugumą, yra skiriami „skaitmeniniams sprendimams“: kovojant su galingais, naujomis technologijomis paremtais įrenginiais, naudojami kiti naujomis technologijomis paremti įrenginiai. Tik menki pinigai skiriami programišiams, jų kultūrai ir mintims, jų ketinimams ir silpnybėms perprasti. Bet kaip surasti programišių? Ir kaip internete išsiaiškinti, ar jūsų naujasis draugas yra programišius, policijos šnipas, žvalgybos agentas, oro pajėgų tyrėjas, pokštininkas, teroristas ar ateivis iš kitos planetos?

Viskas remiasi pasitikėjimu. O stiprinti pasitikėjimą – tai būti kantriam ir puoselėti santykius. Vis dėlto kibernetinio saugumo pasaulyje svarbiausias dalykas yra laikas. Niekur kitur su pasitikėjimu ir laiku susiję sunkumai taip neišryškėjo kaip tada, kai Tamsiosios rinkos buveinė persikėlė iš savo kilmės šalių – Didžiosios Britanijos, Vokietijos ir Jungtinių Valstijų – į šalį, kurios ekonominė ir geopolitinė svarba labai greitai auga – Turkiją.

ANTRA KNYGA

I dalis

26
Bilalas Pitsburge

Pitsburgas, Pensilvanija, 2008 m. vasaris

Vieną gaivų 2008-ųjų žiemos rytą Turkijos policijos inspektorius Bilalas Şenas pro savo kabineto langą įdėmiai žvelgė į Pitsburgo Karšto Metalo tiltą. Pastatytas abipus Monongahilos upės, šiek tiek į dešinę nuo tos vietos, kur ji susilieja su Alegenio upe ir suformuoja didingąjį Ohają, šis tiltas kažkada buvo naudojamas lydytam metalui transportuoti iš šiaurinėje pusėje esančių Elizos lydymo krosnių į pietinės pusės valcavimo staklynus.

Tačiau šiandien inspektorius neturėjo laiko mąstyti apie sniegu padengtą poindustrinę estetiką. Tamsiosios rinkos forumuose jis ką tik perskaitė kai ką, kas sukėlė jam nerimą. Remiantis aiškiai patikima informacija, atėjusia iš Stambulo, inspektoriaus Şeno sekamas nusikaltėlis Cha0 „yra vienas iš didžiųjų vyrukų, turtingas ir galingas“. Jam, turkui, šią frazę nebuvo sunku iššifruoti: jo ieškomas subjektas turi aukštą padėtį užimančių draugų, o tai turkų policininkas suvokė kaip baisiausią košmarą.

Inspektorius Şenas beveik tris mėnesius dirbo Mokymų apie kibernetinių nusikaltimų įrodymus nacionaliniame aljanse. Kai pirmą darbo dieną jis priimamajame laukė, kol jį priims organizacijos

vadovas, čionai atsitiktinai užsuko kaip visada gerai nusiteikęs ir žavus agentas Keithas J. Mularskis. Jis prisistatė ir išgirdęs, kad Bilalas yra iš Turkijos, iš karto pradėjo jam pasakoti viską, ką žino apie garsųjį Tamsiosios rinkos administratorių ir kriminalinio pasaulio meistrą Cha0. Mularskis ir Şenas puikiai sutarė kaip partneriai.

Įėjęs į kabinetą, esantį pastato adresu Technologijos kelias 2000 ketvirtame aukšte, turkų policininkas apstulbo, pamatęs, kaip atrodo ši vieta, nes ji labiau panėšėjo į draudimo kompaniją nei į moderniųjų technologijų fanatikų aplinką, gerai pažįstamą iš tokių televizijos serialų kaip „CSI Niujorkas“. Vienas nuošalus kambarėlis buvo prigrūstas kompiuterinių įkalčių nustatymo prietaisų, įrenginių, galinčių padėti atskleisti giliausias bet kokio skaitmeninio prietaiso paslaptis. Bet šis techninių apžiūrų kabinetas buvo beveik nepastebimas. Jis buvo užantspauduotas, tarsi tam, kad iš užkrėstų tiriamųjų objektų neįsibrautų jokie trojanai ar kokios kitos kenkėjiškos programos. Visi kiti kabinetai buvo tylūs, tvarkingi ir niekuo neišsiskiriantys.

Jau patį pirmąjį rytą Keithas parodė Bilalui savo kabinete esančią rašomąją lentą, kurioje buvo pavaizduota su Tamsiąja rinka susijusių nusikaltėlių piramidė, o jos viršuje buvo užrašytas vardas Cha0. Turkijos policininkas staiga susigėdo. Padedami kolegų iš Didžiosios Britanijos ir Vokietijos, federalai prieš šešis mėnesius buvo pašalinę du energingiausius Tamsiosios rinkos administratorius – JiLsi ir Matricą. Areštai jau buvo įvykdyti Didžiojoje Britanijoje, Vokietijoje, Kanadoje ir Prancūzijoje, o dabar buvo ruošiamasi naujiems suėmimams Jungtinėse Amerikos Valstijose. Taigi pareigūnas iš Ankaros į tai, kad vyrukas iš Turkijos dabar atsidūrė tarp ieškomiausių kibernetinių nusikaltėlių visame pasaulyje, reagavo kaip į sutryptą nacionalinį orumą ir suteptą asmeninę reputaciją.

Turkijos policija, o ypač jos Organizuotų nusikaltimų skyrius, praeitame dešimtmetyje nuėjo ilgą kelią, ir Bilalas buvo pasiryžęs

įrodyti, kad, netgi turėdamas daug mažesnius išteklius nei jo kolegos Vakarų Europoje ir Amerikoje, neseniai Turkijos sostinėje Ankaroje įkurtas Kibernetinių nusikaltimų padalinys yra pajėgus „žaisti aukščiausioje lygoje".

Policijos pareigūnai iš viso pasaulio nuolatos lankydavosi FTB kabinetuose. Jie atvykdavo mokytis iš savo kolegų Amerikoje, bet taip pat ir tam, kad sukurtų tarpusavio paramos tinklus. Įvairių šalių policijos pajėgų bendradarbiavimą paprastai apsunkindavo nepakeliamos biurokratinės procedūros, o asmeninė policininkų draugystė buvo lengviausias būdas jas apeiti.

Bilalas buvo komandiruotas trims mėnesiams. Kaip atvykėlis iš Turkijos, tarp federalų jis buvo naujokas, nors galėjo jiems labai praversti. 2003 m. jis buvo vienas iš dviejų nedidelio Kibernetinių nusikaltimų padalinio steigėjų Turkijos kovos su kontrabanda ir organizuotu nusikalstamumu skyriuje. Deja, palyginti su nusikaltėliais, inspektorius beveik visai neturėjo išteklių.

Savo ruožtu inspektorius Bilalas Şenas norėjo pasimokyti iš FTB. Nepasakysi, kad jam trūko patirties. Į policininkų gretas jis įstojo 1989 m., būdamas penkiolikos užsirašė į varginančius, pačius ilgiausius pasaulyje aštuonerių metų pareigūnų mokymo kursus.

Tai buvo keista, nes dėl savo žemo ūgio ir mąslumo vyresnysis inspektorius labiau priminė turkišką Erkiulio Puaro versiją nei tradicinį kietą Balkanų policininką, kurį įsivaizduojame užgrūdintą kaimo banditų, miesto narkotikų sindikatų ir brutalios baudžiamojo teisingumo sistemos.

Policijos koledžo režimas tikrai buvo sunkus. Tačiau labiausiai Şeną erzino ne spartietiškos gyvenimo sąlygos ir neįtikėtinai sunkios kovinės pratybos, bet visiškas kompiuterių nebuvimas. Nuo mažumės jis naudojosi kiekviena galimybe įslinkti į vaizdo žaidimų automatų pasažus savo gimtajame Eskišechiro mieste, esančiame šiaurinėje Anatolijos pusiasalio dalyje, tarp Stambulo ir Ankaros.

Būdamas vos šešerių, jis atsitiktinai užtiko žaidimą „River Raid"*. Kiekvieną laisvą minutę Bilalas praleisdavo skraidindamas virš upės dvimatį naikintuvą ir šaudydamas mažus sraigtasparnius, laivus, tankus ir dirižablius ir tuo pat metu mėgindamas papildyti lėktuvą degalų. Prikaustytas prie tos paslaptingos pasikartojimų ir retsykiais pasitaikančių apdovanojimų sekos, kuri neleidžia atsitraukti nuo kompiuterio ekrano daugeliui vaikų, paauglių ir jaunuolių, Bilalas buvo užsikrėtęs tokia pat žaidimų manija kaip ir daugelis pirmųjų to paties amžiaus programišių. Jį, kaip ir kitus, traukė tas pat ryžtas laimėti.

Galbūt šis užsispyrimas ir padėjo naujokui gavus pirmąjį paskyrimą į kaimo policijos nuovadą kažkur Anatolijos pusiasalio viduryje. Nors buvo praeito amžiaus paskutinio dešimtmečio vidurys, vienintelis ten esantis prietaisas buvo senovinė mechaninė rašomoji mašinėlė. Liudytojų parodymų užrašinėjimą šia mašinėle Bilalas laikė nesuderinamu su pareigūno orumu, tačiau buvo taip pasiryžęs pagerinti savo spausdinimo įgūdžius, jog praleido daugybę valandų barškindamas klavišus. O kai to nedarydavo, šis nuostabus savamokslis mokėsi mandarinų kalbos.

Kai Bilalas kreipėsi dėl darbo Ankaros elitiniame Organizuotų nusikaltimų padalinyje, viršininkas jo paklausė, kam jis mokosi kinų kalbos. „Kai Kinija atidaro duris išoriniam pasauliui, – atsakė jis, – Organizuotų nusikaltimų skyriuje mums greitai gali prireikti pareigūnų, kalbančių mandarinų kalba." Šiuo atsakymu jis palenkė viršininką į savo pusę ir gavo darbą.

Atvykęs į Turkijos sostinę, jaunasis detektyvas parašė prašymą studijuoti Ankaros universitete, norėdamas gauti magistro laipsnį – vėlgi savo iniciatyva ir savo laisvu laiku. Jis pasirinko Turkijoje nežinomą ir netyrinėtą temą – „Elektroninio valdymo galimybės ir

* Antskrydis virš upės. (Angl.)

rizika“ – ir savo darbe nagrinėjo ryšius tarp privatumo, pilietinių teisių ir kibernetinių nusikaltimų.

Bilalas Şenas pradėjo tyrinėti internetinių nusikaltimų paplitimą savo šalyje, nes buvo vienas iš tų Turkijos policininkų, kurie pajėgūs tai padaryti. Kitos valstybinės tarnybos, taip pat jau įsisąmoninusios kibernetinio saugumo strateginę svarbą, buvo karinės ir civilinės žvalgybos agentūros, bet jos, aišku, niekada nereklamavo savo gebėjimų ar motyvų.

Kartu su savo kolega Bilalas apsiėmė padaryti Heraklio vertą darbą – įtikinti gremėzdišką Vidaus reikalų ministeriją dalį savo vertingų lėšų skirti Kibernetinių nusikaltimų padaliniui. Prašymams, įtikinėjimams ir politikavimui prireikė trejų metų. Laimei, jo kolega buvo įvaldęs osmanų meną rasti tinkamą toną, kalbant su atitinkamais Vidaus reikalų ministerijos biurokratais.

Kaip ir visi kovos su kibernetiniais nusikaltimais padaliniai, besikuriantys prie policijos pajėgų visame pasaulyje, naujasis Turkijos skyrius galėjo pasinaudoti tuo faktu, kad iš esmės niekas daugiau ministerijoje nesuvokė tamsiosios kompiuterių pusės. Gavę leidimą veikti, du vyrai pasijuto savotiškai laisvi nuo išorinio kišimosi, nes niekas kitas neturėjo jokio supratimo, kuo jie užsiima, o ir valstybės iždui jie nebuvo didelė našta.

Nors inspektoriaus vyresnybė ne ką išmanė apie jo darbą, kolegos toli už Atlanto greitai pastebėjo jo laimėjimus. Kai policija Vokietijoje ir Britanijoje 2007 m. vasarą suėmė Tamsiosios rinkos administratorius Matricą ir JiLsi, Turkijos kovos su kibernetiniais nusikaltimais komanda įkalino vieną iš garsiausių kibernetinių nusikaltėlių – Maksiką. Svarbus Tamsiosios rinkos veikėjas (kartu su kitais jis aprūpindavo prancūzų programišių iš Marselio Lordą Kaisersose'ą vogtais kreditinių kortelių duomenimis) Maksimas Jastremskis iš šiaurės rytų Ukrainos miesto Charkovo manė, kad bus saugus Turkijoje, nes ten ne tik niekada nebuvo suimtas nė vienas

kibernetinis nusikaltėlis, bet ir Ukrainos ir Turkijos santykiai, ypač nusikaltėlių pasaulyje, buvo kaip niekada nuoširdūs.

Be to, ukrainiečiai dievino šią šalį dėl jos žavios pakrantės – puikūs Antalijos paplūdimiai tapo abiejų šalių kibernetinių vagišių privaloma ir madinga kelionių vieta.

JAV slaptoji tarnyba persekiojo Maksiką dvejus metus. Iki 2006 m. jie jau buvo sėkmingai išvogę paslaptis iš jo nešiojamojo kompiuterio, o paskui surengę jo susitikimus su Slaptosios tarnybos agentais Tailande, Dubajuje ir Turkijoje. Praeityje bendradarbiavimas su turkų policija buvo nesėkmingas, jei ne visiškai neįmanomas. Bet suėmusi Maksiką, besilepinantį kaitrioje Antalijos saulėje, Turkijos policija paskleidė žinią, kad labai trokšta bendradarbiauti kibernetinių nusikaltimų srityje ir kad išmano, kaip tai padaryti.

Nors šio pasaulio JiLsi ir Matricos daugiau nebesireiškė Tamsiosios rinkos forumuose, likusi komanda vis dar buvo aktyvi – iš tiesų Tamsioji rinka vėl patyrė kriminalinės veiklos pakilimą. Ironiška, bet akstiną šiam atgimimui suteikė kito kibernetinio nusikaltėlio – Ledo Žmogaus – suėmimas.

2007 m. rugsėjį JAV teisėsaugos pareigūnai galiausiai atsekė Maksą Viziją jo slaptame bute San Fransisko centre. Netekusi Ledo Žmogaus, subyrėjo Karderių rinka, taigi tuo metu, kai Rusijos karderių sceną valdė Mazafaka, Tamsioji rinka buvo neginčytina lyderė tarp anglakalbių kibernetinių nusikaltėlių. Tiesiogiai ar netiesiogiai ši svetainė kiekvieną mėnesį vis dar uždirbdavo šimtus tūkstančių svarų nelegalaus pelno ir tarp karderių ir programišių išliko tokia pat populiari kaip visada.

Tamsiojoje rinkoje dabar buvo trys pagrindiniai veikėjai: Cha0, Meistras Splyntras ir Štirlicas. Greitai prie jų turėjo prisidėti paslaptingasis Lordas Cyrikas. Lordo Cyriko dalyvavimas kardingo scenoje tarp karderių sulaukė tiek pat priešiškumo, kiek ir šlovinimo. Tie, kurie jo neapkentė, manė, jog jis yra FTB informatorius Mularskis,

nors taip pat būta įtarimų, kad Meistras Splyntras ir Štirlicas iš tiesų arba dirba JAV teisėsaugoje, arba su ja bendradarbiauja. Vienintelis dalykas, dėl kurio sutarė tiek policininkai, tiek programišiai: rimčiausias forume likęs nusikaltėlis yra Cha0.

Nors kitų Tamsiosios rinkos narių dosjė buvo sukaupta daugybė įrodymų, apie Cha0 Mularskis ir Şenas žinojo tik du pagrindinius faktus: jis gyvena Stambule ir turi klestintį kreditinių kortelių amžiaus pagrindinių sukčiavimo įrankių – nelegalių skaitytuvų – verslą. Tačiau detektyvai nežinojo nei tikrojo Cha0 vardo, nei jo gyvenamojo adreso, nei IP adreso, nei jokių jo kompanionų. Arba Cha0 niekada neegzistavo (tai neįmanoma), arba jis niekada nedarė klaidų.

Jei pastarasis atvejis būtų tiesa, tai reikštų, jog Cha0 taip ištobulino savo skaitmeninių pėdsakų maskavimo sistemą, kad kriminalistikos pėdsekiams tapo neįmanoma tiksliai nustatyti jo buvimo vietos. Dalį tos maskavimosi sistemos buvo suteikęs Grendelis, laisvalaikiu padedantis Tamsiajai rinkai (žinoma, už užmokestį). Ironiška, kad Grendelis taip pat teikė vadinamąsias „apvalkalo“ sistemas, kurios maskuodavo Mularskio serverių buvimo vietą. Teikti Tamsiajai rinkai šias paslaugas jo pirmiausia paprašė JiLsi – realiame gyvenime Grendelis dirbo informacinių technologijų apsaugos kompanijoje Vokietijoje. Keista, bet kažkaip atsitiko, kad, pradėjęs nuo Tamsiosios rinkos, jis galų gale interneto svetainėje siūlė apsaugos paslaugas ir nusikaltėliams, ir policininkams.

Nors ir labai stengėsi, Bilalui Şenui nesisekė priderinti Cha0 stiliaus nė prie vieno žinomo Turkijos nusikaltėlio braižo. Atrodė, kad šioje asmenybėje susilieja du esminiai interneto tamsiosios pusės aspektai: jis buvo kompiuterių fanatikas, turintis nepaprastų techninių įgūdžių, bet kartu ir talentingas nusikaltėlis, kuriam rūpi menkiausia smulkmena ir kuris nieko nepalieka atsitiktinumui. Taip pat buvo tikėtina, kad Cha0 – tai kolektyvinis gerai organizuoto

sindikato slapyvardis, nors lingvistinė analizė primygtinai teigė, jog skelbimus ir žinutes internete iš tiesų formuluoja tik vienas žmogus.

Taigi, kai Bilalas gavo iš Stambulo pranešimą, kad Cha0 „yra vienas iš didžiųjų vyrukų", jis ne tik susirūpino, bet ir suprato, kad nuo šios akimirkos turės elgtis atsargiai net ir tokioje greitai modernėjančioje šalyje kaip Turkija.

Atėjus naujam tūkstantmečiui, Turkija darėsi kaskart patrauklesnė programišių, įsilaužėlių ir kitų kibernetinių nusikaltėlių susitikimų vieta. Praeito amžiaus paskutinio dešimtmečio pabaigoje kibernetinė kriminalinė veikla susibūrė tam tikruose vadinamųjų BRIC šalių regionuose. Ekonomistas iš „Goldman Sachs"* šiuo trumpiniu pavadino pirmaujančias naujai atsirandančių rinkų šalis: Braziliją, Rusiją, Indiją ir Kiniją, antrąjį pasaulinės galios turintį junginį po Didžiojo aštuoneto šalių (G 8), nors politiškai Rusija priklauso abiem junginiams.

BRIC šalys pasižymi svarbiomis bendromis socialinėmis ir ekonominėmis charakteristikomis. Visų jų ekonomika padarė pažangą ir suklestėjo po kelių sąstingio dešimtmečių. Šios šalys turi daug gyventojų ir jų suvienytomis pastangomis pasiekė didelį vystymosi tempą. Tuo pat metu gyvybingo, o kartais ir agresyvaus nacionalizmo atgimimas padėjo joms įgyti veiklių pasaulinio lygio veikėjų statusą. Jų švietimo sistema siūlo puikų pagrindinį išsilavinimą. Tačiau ypatinga turtinė nelygybė pagimdė naują vargingų ir neturinčių darbo jaunų žmonių klasę, kuri, priešingai ankstesnėms kartoms, turi didelių materialinių troškimų, nes šie jaunuoliai gerai įsiminė vartotojišką informaciją, kuri yra esminė globalizacijos dalis. Norėdama įgyvendinti šiuos siekius, nedidelė dalis jaunuolių pradėjo entuziastingai darbuotis interneto kavinėse, neatpažįstamai pasislėpę

* „Goldman Sachs Group Inc." – pelningiausias visų laikų Volstrito investicinis bankas.

nuo teisėsaugos ir visų kitų. Ten jie atrado nesuskaičiuojamą daugybę internetinių galimybių mokytis, kaip įsilaužti į kompiuterius.

Turkija buvo laikoma BRIC garbės nare, nes jos ekonomika, palyginti, pavyzdžiui, su Rusijos, atrodė daug dinamiškesnė. Ši valstybė turi apie aštuoniasdešimt milijonų gyventojų ir jos augimo tempai didėjo netgi sparčiau nei tikrųjų BRIC šalių. Visi pripažino jos strateginę svarbą – ji glaudžiasi prie Juodosios ir Viduržemio jūrų ir turi sienas su Bulgarija, Graikija, Iranu, Iraku, Sirija ir Armėnija, – vargu ar rasi kaimyną, kuris per pastaruosius du dešimtmečius nebūtų patyręs rimtos suirutės ar karo. Turkijos politika visada buvo neprognozuojama, bet, perėjus į naują tūkstantmetį, auganti ekonominė galia ir patirtis išryškino jos pagrindinį vaidmenį keliuose gyvybiškai ir strategiškai svarbiuose geografiniuose regionuose: Artimuosiuose Rytuose, Centrinėje Azijoje, Juodosios jūros regione ir Balkanuose.

Praeito amžiaus paskutiniame dešimtmetyje šalies interneto infrastruktūra vystėsi lėtai, tačiau pastaraisiais metais pradėjo vytis kitas šalis. Ekonominis Turkijos variklis Stambulas pirmavo pagal sėkmingai steigiamas naujas įmones, tarp jų ir pelningas projektavimo, žiniasklaidos ir serviso kompanijas.

Kita vertus, šalies dydis, jos gerėjanti infrastruktūra ir vidurinės klasės jaunimo švietimas atvėrė galimybes kibernetiniams nusikaltimams. Iki tol, kol 2005 m. susikūrė ir pradėjo rimtai dirbti Bilalo Şeno skyrius, nedaug buvo daroma, kad programišiams ir įsilaužėliams būtų užkirstas kelias reikštis internete pačioje Turkijoje, nesibijant būti atpažintiems. Kibernetinių nusikaltimų padalinys ėmė keisti situaciją, bet tai buvo varginanti kova. Jei inspektorius Şenas būtų sugebėjęs atsekti Cha0, tai būtų buvęs svarbus jo skyriaus laimėjimas.

Tačiau visai prieš pat 2008 m. kovo vidurį, kai inspektorius turėjo grįžti iš Pitsburgo į Turkiją, jis sulaukė kito perspėjimo apie

pavojų, ir šis perspėjimas dar labiau apsunkino jo tyrimą, susijusį su Cha0. Šį sykį žmogus iš Stambulo, palaikantis ryšį su inspektoriumi, pateikė gluminančio interviu detalių. Interviu gerai žinomai naujienų agentūrai „Haber 7" davė turkų programišius vardu Kieras. Jis prisipažino išsisukęs nuo įstatymo.

„Haber 7" autoritetas iš dalies buvo paremtas dvasiniu palaikymu, kurio ši agentūra sulaukė iš didžiulio vietinių islamistų judėjimo, vadinamo Güleno judėjimu, skelbiančio į Jungtines Valstijas pasitraukusio savo lyderio Fethullaho Güleno filosofiją. Kaip bendruomenės naujienas pateikianti organizacija, „Haber 7" aiškiai simpatizavo valdančiajai AK partijai*, kuri, nors ir proislamiška, visgi buvo demokratinė.

Jaunasis programišius Kieras kreipėsi į naujienų agentūrą, norėdamas pareikšti, kad jis ne tik pažįsta Cha0, bet ir, kaip jis leido suprasti, žmogų ar žmones, pasislėpusius už paties sėkmingiausio Tamsiosios rinkos paslaptingojo avataro ir planuojančius dar labiau išplėsti savo kriminalinę imperiją. Prie straipsnio buvo pridėta ir programišiaus nuotrauka, padaryta jam kalbant Stambulo kavinėje. Fotografuota iš nugaros, bet šiek tiek matėsi ir programišiaus profilis.

Bilalas tada dar nežinojo, kad tas programišius yra jaunas žmogus vardu Mertas Ortaças. Buvo manoma, jog šis keistas veikėjas bendrininkauja su kitu kibernetiniu nusikaltėliu vardu Cryptos, kuris 2008 m. sausį buvo suimtas, įtarus, jog įsilaužė į vieną iš didžiausių Turkijos finansinių institucijų – banką „Akbank". Daugeliu atžvilgių „Akbank" atvejis buvo dar rimtesnis nei Tamsiosios rinkos, nes komanda iš tiesų įsibrovė į pagrindinę banko sistemą, pasinaudojusi jos operacinės sistemos silpnybėmis. Bet nei Stambu-

* Teisingumo ir vystymosi partija (turk. *Adalet ve Kalkınma Partisi*), sutrumpintai AK partija, yra Turkijos dešinioji centristinė konservatorių politinė partija.

lo policija, nei Kovos su organizuotu nusikalstamumu skyrius neturėjo nė mažiausio supratimo, kur slepiasi Ortaças. Ir staiga jis pats pasirodė ir kalbėjosi su žurnalistais.

Nors ir buvo sekamas tiek Stambulo policijos, tiek būrio žvalgybos agentų, Ortaças laikraščio korespondentams pasakė, kad 2007 m. gruodį jis išsisuko nuo visų persekiotojų ir perėjo į pogrindį. Iš ten išlindo tik sykį, kad savo keistą ir fragmentišką istoriją papasakotų laikraščiui.

Stambulo policija jautėsi sumišusi dėl jo epizodinio pasirodymo. Jo interviu prasmė kėlė susirūpinimą: labai jau lengvai jis išvengė suėmimo. Dar labiau apsunkindamas policijos vargus, programišius perspėjo juos, kad areštai, susiję su „Akbank" atveju, neturės įtakos Turkijos bankų saugumui, nes bankus dabar apiplėšinėja dar grėsmingesnis nusikaltėlis, kuris siekia pasisavinti kuo daugiau pinigų, o jo vardas yra Cha0. (Bilalas Şenas, be abejo, buvo girdėjęs apie Cha0, bet tai buvo pirmas kartas, kai paslaptingas vyriškis apie jį prabilo viešai.)

Ortaças pareiškė, kad Cha0 yra saugomas vyriausybės pareigūnų. Interviu bent jau patvirtino Şenui, kad Cha0 iš tiesų egzistuoja. Vis dėlto skaitydamas jį inspektorius jautėsi žvelgiąs į bedugnę. Kas galėtų ginti Cha0 ir kodėl?

27
Svarbiausias portalas

Pakėlęs akis nuo savo užrašų, inspektorius Şenas pajuto, kaip jo nuogąstavimai perauga į baimę. Dabar paaiškėjo, kad, atsakydamas į Ortaço interviu, Cha0 pats pasiuntė pranešimą naujienų kanalui „Haber 7“. Tai buvo neeilinis protrūkis, pagardintas stipriais didybės manijos pliūpsniais ir tvirtu įsitikinimu. „Aš esu pagrindinis teisės sergėtojas Tamsiojoje rinkoje, – griaudėjo jis. – Aš užkertu kelią farų ir plėšikų darbeliams. Aš kuriu taisykles, kurioms visi turi paklusti.“

Pasinaudojęs savo ryšiais, inspektorius greitai nustatė, kad Cha0 iš tiesų gali būti nepasiekiamas įstatymui. Şenas pasikalbėjo su savo seniausiu draugu iš Stambulo policijos ir išgirdo bauginančių dalykų: abiem vyrams kėlė rūpestį tai, kad Cha0 pačioje policijoje gali turėti slaptą informacijos šaltinį, kuris akivaizdžiai praneša savo bosui apie tyrimo eigą. Jeigu jie negali pasitikėti savo komanda, savo pastiprinimu, o svarbiausia – savo viršininkais, tai kaip jie galėtų pastūmėti bylą bent kiek į priekį?

Savo pirmajame interviu Mertas Ortaças daug kalbėjo apie slaptąją policiją ir kitas pajėgas, dirbančias prie Tamsiosios rinkos bylos. Kai kuriose šalyse tai gal kvepėtų sąmokslu ir paranoja, bet Turkijoje būtų buvę neprotinga į tai neatsižvelgti. Mertas davė suprasti, kad visa Tamsiosios rinkos veikla galėtų paliesti žmones, turinčius pačią didžiausią ekonominę, karinę ar politinę galią.

Sudėtinga šalies politinė struktūra įgijo naują formą, kai po 2002 m. rinkimų AK partija tapo valdančiąja. Žinant, kad daugiau

nei 90 procentų turkų yra musulmonai, tai, kad aiškiai islamiška partija laimėjo triuškinančią pergalę, pats savaime nieko nestebino. AK partija primygtinai tvirtino, kad jos religiniai įsitikinimai yra antraeiliai, palyginti su įsipareigojimais demokratijai, panašiai kaip daugelis Europos nuosaikiųjų konservatorių partijų save vadina krikščionimis demokratais.

Bet Turkija puoselėja kitą neaprėpiamos galios turinčią ideologinę tradiciją – kemalizmą. Pagrindinis šio judėjimo, pavadinto šiuolaikinės Turkijos įkūrėjo Kemalio Atatürko vardu, principas siūlo visiškai atskirti Bažnyčią nuo valstybės. Visur – parduotuvėse, namuose, kontorose, kareivinėse, ligoninėse ir kalėjimuose – kabantys paveikslai su Atatürko atvaizdu atspindi didžiulę turkų pagarbą jo sekuliarizacijos idėjoms (kaip ir baimę būti suimtiems, jei jų nepaisys).

Tačiau kemalizmas turi įvairių formų. Du aistringiausi jo šalininkai yra kilę iš pasaulietinio vidurinės klasės elito. Tai intelektualai, kvalifikuoti specialistai ir valstybės tarnautojai iš vienos pusės ir vadinamoji „giluminė valstybė“, arba „valstybė valstybėje“, iš kitos. Abu šie kemalizmo šalininkai įtariai žiūri tiek į AK partiją, tiek vienas į kitą.

„Valstybė valstybėje“ – taip grėsmingai vadinamas karinis-pramoninis kompleksas, kuris pokario laikotarpiu veikė kaip pagrindinis Turkijos politikų arbitras. Būdama viena iš dviejų NATO narių, turinčių sieną su Sovietų Sąjunga (kita tuo metu buvo Norvegija), šalis vaidino pagrindinį vaidmenį šaltajame kare, o jos sąjungininkai, vadovaujami JAV, džiaugėsi galėdami apsimesti nepastebį milžiniškos karinės naštos, užkrautos tų šalių gyventojams.

Nuolat kišdamasi į politinį gyvenimą, ši Turkijos saugumo institucija buvo taip giliai suleidusi nagus į šalies ekonomiką, kad kartais būdavo sunku atskirti grobuonį nuo jo aukos. Ji gynė šiuos painius ir pelningus santykius, naudodamasi kemalizmo idėjomis: jei atrodė,

kad trapi demokratinė tvarka kelia grėsmę jos verslo interesams, įsikišdavo kariškiai ir pareikšdavo, jog atsirado poreikis ginti Atatürko paveldą. Pagal tradiciją ginkluotosios pajėgos niekam neleisdavo pasimaišyti jų kelyje. Būtų galima perfrazuoti seną turkų posakį: „Sukirsk rankomis su „valstybe valstybėje", ir ji nutrauks tau ranką."

Tačiau maždaug penkiolika pastarųjų metų Turkijos vyriausybės viena po kitos pradėjo reformas, iš dalies siekdamos atitikti Europos Sąjungos narystės kriterijus. Nepaisydami baimės dėl slaptų ekstremistinių islamizmo tikslų, naujieji AK vadai prastūmė kai kuriuos liberaliausius pokyčius turkų visuomenėje, pavyzdžiui, panaikino mirties bausmę. Kitas bandymas sustiprinti teisinės valstybės viršenybę buvo AK partijos pastangos atskirti reguliariąsias policijos pajėgas nuo kariškių.

Šis procesas sukėlė tam tikrų puikių ir labai teigiamų pokyčių. Dalis valstybinių tarnybų pradėjo suprasti, kad pagrindinis jų darbas yra ne pelnytis, naudojantis savo tarnybine padėtimi, bet tarnauti paprastiems žmonėms. Taip pat jos pradėjo įsisąmoninti, kad būdama galinga, Turkijos valstybė sustiprins savo tarptautinę įtaką ir savo autoritetą.

Tačiau lėtas naujosios Turkijos gimimas nebuvo beskausmis procesas, o ir jo pasekmių niekas negalėjo numatyti. Šį procesą lydėjo nuožmi politinė kova, kuri bet kam, sąmoningai ar nesąmoningai įsipainiojusiam į netvirtas neaiškių jėgų sąjungas, galėjo baigtis mirtimi.

Pagrindinė karo tarp šių jėgų scena oficialiai buvo atidaryta 2007 m., prasidėjus vadinamiesiems Ergenekono tyrimams. Ergenekono vardu, žinomu iš pamokomos epinės senovės turkų legendos, pastaruoju metu buvo pavadinta konspiracinė „valstybės valstybėje" organizacija, kurioje vadovaujantieji kariuomenės, žvalgybos ir politikos veikėjai bendradarbiavo su organizuoto nusikalstamumo atstovais, žurnalistais, teisininkais ir kitais specialistais. Manoma, kad

jų tikslas buvo apriboti demokratiškai išrinktų vyriausybių, ypač AK partijos, įtaką. Tačiau, remiantis prokurorų ir vyriausybinės žiniasklaidos teiginiais, šio sąmokslo nariai nuėjo dar toliau – 2009 m. jie planavo karinius veiksmus, kurie padėtų atkurti „valstybės valstybėje" viršenybę prieš išrinktąją vyriausybę.

Nuo 2007 m. policija per vadinamąjį Ergenekono tyrimą suėmė šimtus aukštesniųjų kariškių ir žvalgybos veikėjų. Tačiau tuo pat metu ji suėmė ir daugybę žurnalistų ir teisininkų, apkaltinusi juos dirbus Ergenekonui už pinigus arba dėl ideologinių paskatų. Nedidelė, bet iškalbinga liberalių intelektualų klasė ir kiek didesnė vidurinė klasė perspėjo, kad demokratinė vyriausybė ėmėsi tam tikrų bauginimo priemonių, kurios paprastai būdingos „valstybei valstybėje". Kaltinimai Ergenekonui pagal laiko dvasią daugiausia buvo paremti skaitmeniniais įrodymais, demonstruojančiais augančius vietinės žvalgybos tarnybų kibernetinius gebėjimus: slaptu mobiliųjų telefonų klausymusi, keitimosi žinutėmis programų pranešimais, kompiuteriniais failais.

Bilalas Şenas su visais šiais dalykais niekaip nebuvo susijęs, tik dėl savo stropumo, atsidavimo ir jaunatviškos energijos buvo labiau linkęs palaikyti naujai užgimstančią Turkiją nei senąją. Vis dėlto, kaip ir dauguma turkų, jis puikiai suprato, kokiomis sudėtingomis politinėmis aplinkybėmis jam, kaip ir visiems kitiems, tenka dirbti. Bet kuris Turkijos policininkas mažiausiai troško tapti nekalta marionete, sutraiškyta kovoje tarp „valsybės valstybėje" ir demokratiškai sudarytos vyriausybės. Beveik visi turkai kiek galėdami vengė viešų diskusijų apie Ergenekoną. Tačiau visi žinojo, kad daugelio pagrindinių kriminalinių bylų tyrimai buvo susiję su Ergenekonu, nesvarbu, ar šios bylos turėjo akivaizdžią politinę prasmę, ar ne.

Bilalui teko būti atsargiam, bet jis nesiruošė mesti medžioklės.

Dar būdamas Pitsburge jis labai susidraugavo su Mularskiu, o FTB agentas pasidalijo su juo visa turima informacija apie Cha0.

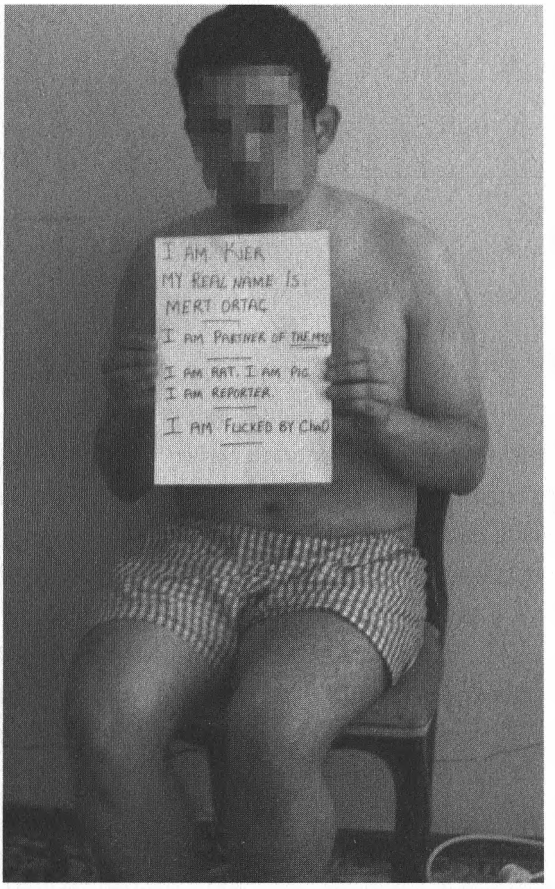
Dviese jie pradėjo rinkti duomenis savo negausiai dosjė. Būdamas vienu iš pagrindinių Tamsiosios rinkos veikėjų, Mularskis galėjo naudotis savo milžinišku archyvu, o Şenas mokėjo skaityti turkiškai. Inspektorius norėjo įvertinti Cha0 asmenybę ir pažiūrėti, ar ji panaši į kokį nors žinomą Turkijos kibernetinį nusikaltėlį: buvo nuskenuota daugybė dokumentų, keliaujančių pirmyn ir atgal tarp Ankaros, Stambulo ir Pitsburgo.

Jau ir taip ganėtinai painūs reikalai dar labiau susipainiojo po to, kai inspektorius Şenas grįžo namo į Ankarą. Internete cirkuliavo paslaptingas paveikslėlis.

Biļalas sunkiai tramdė pyktį ir nusivylimą. Agentas Mularskis jam atsiuntė nuotrauką, kuri buvo pasirodžiusi „Haber 7" interneto svetainėje, o paskui ir San Fransiske leidžiamame žurnale *Wired*. Paslaptingas vyriškis vardu Kieras sėdėjo ant kėdės tik su apatinėmis kelnaitėmis ir, reikia manyti, priverstinai laikė iškėlęs popieriaus lapą, kuriame buvo užrašyta:

1. AŠ ESU KIERAS. MANO TIKRASIS VARDAS MERTAS ORTAÇAS.
2. AŠ BENDRADARBIAUJU SU ŽINIASKLAIDA.
3. AŠ ESU ŽIURKĖ. AŠ ESU PARŠAS.
4. AŠ ESU INFORMATORIUS.
5. Cha0 MANE VEDŽIOJA UŽ NOSIES.

Pusė Stambulo policijos pajėgų bergždžiai ieškojo Kiero, arba Merto Ortaço, jei vadinsime jį tikruoju vardu, tačiau Cha0 pavyko ne tik jį atsekti, bet net pagrobti ir pažeminti. Visai tikėtina, kad šio žmogaus gyvybei gresia pavojus. Viešpatie, kas gi čia vyksta?



Bilalui Şenui buvo visiškai aišku, kad bet ką, kas susiję su internetu, priimti už gryną pinigą nėra išmintinga. Kaip patyręs kriminalinių forumų naršytojas ir žmonių elgesio internete tyrinėtojas, jis žinojo, kad meluoti, sukčiauti, perdėti faktus, apgaudinėti ir regzti sąmokslus internete yra įprasta. Tačiau „DarkMarket" istorija Europoje, o ypač Turkijoje, peržengė šias kasdien pasitaikančias veidmainystes ir peraugo į nerealaus masto machinacijų, šnipinėjimo ir išdavysčių istorijas. Ir joms nebuvo galo.

II dalis

28
Ciao, Cha0

Iš savųjų Tamsiosios rinkos tyrimų, atliktų kartu su Keithu Mularskiu, inspektorius Şenas žinojo, kad Cha0 turi savo interneto svetainę „CrimeEnforcers.com“ (pavadintą „Nusikaltimų vykdytojai“, parodijuojant frazę „įstatymų vykdytojai“ (angl. *Law Enforcers*), kuri tarp nusikaltėlių jau seniai buvo sutrumpinta į LE, nes buvo labai dažnai vartojama internetinėse diskusijose).

Svetainės „CrimeEnforcers“ pradiniame puslapyje Cha0 išaiškino jos tikslus ir teikiamas paslaugas:

> Mes esame privati organizacija, sukurta jūsų specialiems tobulėjimo poreikiams. Mūsų sritis – elektronika ir kompiuterių inžinerija. Jei jums reikia specialios techninės (ypač modernių technologijų) ar programinės įrangos, kurios jūsų šalyje negalima pagaminti ar net apie tai diskutuoti dėl bet kokių, pavyzdžiui, teisinių priežasčių ir t. t., tada jūs atsidūrėte ten, kur reikia.
>
> Mes siūlome visiškai anoniminį jūsų projektų įgyvendinimą užsienyje. Mums nerūpi, ką jūs norite daryti su technine ir programine įranga, kurią mes pagaminsime pagal jūsų pageidavimą.

Savaime suprantama, kad mums labai svarbus jūsų privatumas ir mes jo niekam neatskleisime, kad ir kokios būtų priežastys. Mums nereikia jūsų pavardės, adreso ir t. t. Mums reikia tik jūsų elektroninio pašto adreso. Jūs gausite sertifikatą ir kodą, kad galėtumėte saugiai prisijungti prie mūsų privataus forumo ir sekti savo užsakymo vykdymą ir netgi užduoti klausimus prie jūsų projekto dirbantiems inžinieriams.

Jei radote šią interneto svetainę, vadinasi, jau žinote mus. Mes nesame pigūs vykdytojai ir negalime būti jūsų partneriais. Jei norite, kad jūsų svajonės išsipildytų, turite turėti pakankamai pinigų, kuriuos galėtumėte investuoti į savo svajones. Jums netgi teks sumokėti už prašymą apskaičiuoti jūsų projekto kainą.

Kai jau priprasite prie jo šiek tiek darkytos supaprastintos anglų kalbos, vadinamos *Globish**, jums paaiškės Cha0 verslo planas. Jis siūlė logistikos paslaugas ir paramą tiems, kas nori išsiaiškinti karjeros galimybes kibernetinių nusikaltimų srityje. Užuot pats daręs nusikaltimus, jis padėjo užsiimti šia praktika mažiau įgudusiems kompiuterių vartotojams. Kompiuteriniai nusikaltimai pradėjo mėgdžioti realaus pasaulio modelius.

Kituose svetainės „CrimeEnforcers.com“ tinklalapiuose buvo galima pamatyti Cha0 gaminius. Jo pagrindinis produktas buvo kreditinių kortelių duomenų nuskaitymo prietaisas – nelegalus skaitytuvas, ir jau netrukus jo teikiama paštu užsakomų skaitytuvų paslauga suklestėjo ir tapo reikšmingu verslu.

* *Globish* (sutr. *global English* – pasaulinė anglų k.) yra formalizuota anglų kalbos pokalbė, kuriai būdinga supaprastinta standartinė anglų kalbos gramatika ir 1 500 žodžių. Jos autorius teigia, kad iš esmės tai nėra kalba, o tik tam tikras bendras pagrindas, kurį neanglakalbiai pritaiko savo tarptautiniams verslo reikalams.

„CrimeEnforcers" taip pat siūlė nešiojamuosius kreditinių kortelių nuskaitymo prietaisus – portatyvinius įrenginius, naudojamus pardavimo ar atsiskaitymo vietose, panašius į tuos, kuriuos matote daugelyje restoranų. 2007 m. pradžioje policininkai keliose Anglijos vietose atskleidė tinklą degalinių darbuotojų, kurie buvo urmu prisipirkę šių prietaisų. Manoma, kad jie gavo jų arba iš Tamsiosios rinkos nario kanadiečio Drono, arba iš Cha0 įmonės. Kai klientas paduodavo savo kreditinę kortelę, darbuotojas po prekystaliu mikliai nuskaitydavo ją nelegaliu skaitytuvu, įrašydavo jos duomenis, o tada nuskaitydavo legaliu prietaisu.

Tie, kurie žengė pirmuosius neužtikrintus žingsnius kibernetinių nusikaltimų erdvėje, svetainėje „CrimeEnforcers" rado daugybę naudingų patarimų, galinčių labai palengvinti šį procesą. Visiškiems naujokams „CrimeEnforcers" siuntė naudingus filmukus, kuriuose animacinis veikėjas Cha0, kalbantis elektroniniu balsu, visgi išduodančiu savitą realaus žmogaus tembrą ir melodingumą, dalijo patarimus ir nurodymus, kaip, planuojant įvykdyti nusikaltimą, pasirinkti tinkamiausius bankomatus.

Pavyzdžiui, žiūrovams jis aiškino, kad įdiegti nelegalius skaitytuvus į bankomatus ten, kur yra daug nelegalių imigrantų, nėra gera mintis (bankomatuose nėra didelės pinigų apyvartos, juos stebi daug smalsių akių ir sukiojasi per daug konkuruojančių nusikaltėlių). Vietoj to jis siūlė išdėstyti juos netoli naktinių klubų, „kur turtuolių vaikai dažnai naudojasi savo tėvų kreditinėmis kortelėmis".

Patikimo kriminalinės pramonės tiekėjo Cha0 vardas greitai išpopuliarėjo internete, taigi jam tapo itin svarbu sutvirtinti savo autoritetą ir likti neatpažintam.

Bendraujant paprastai buvo vartojama *Globish* – antrinė darkyta anglų kalba, kuri plačiai paplito kaip žargonas internete, tarsi koks bendras šifras, leidžiantis brazilams bendrauti su korėjiečiais ar bulgarams su indoneziečiais. Greitai jos rašyba ir vartojimas internete

netgi tarp tų, kuriems anglų kalba gimtoji, pradėjo vystytis įvairiomis savitomis kryptimis. Buvo galima bandyti įspėti žinutės autoriaus kilmę, tačiau paprastai bent kiek tiksliau nustatyti jo tautybės buvo neįmanoma.

Visai kas kita – rusų ir kinų kalbos. Rusakalbių kriminalinių svetainių dalyviai savo komentaruose gausiai vartoja vietinį žargoną, kurį kai kurie kalbininkai gal ir galėtų suprasti, bet tik patys talentingiausieji įstengtų atkartoti ir likti neatpažinti, kad kalba ne savo gimtąja kalba. FTB agentai anglakalbių forumuose sugebėdavo ir visai neišsiduoti, bet rusų forumuose jiems sunkiai pavykdavo netgi pirmą sykį įsiregistruoti. Nors JAV teisėsaugos ir žvalgybos pareigūnai kartais naudodavosi gimtąja kalba kalbančių rusų ar kinų paslaugomis, jie, be abejo, niekada neturėjo galimybės tiek priartėti prie finansinių ir lingvistinių šaltinių, kad galėtų kontroliuoti rusų svetaines taip, kaip iš dalies sugebėjo tai daryti su Tamsiąja rinka.

Tačiau anglakalbių svetainėse buvo daug sunkiau nustatyti tikrąją pašnekovo tapatybę. Internetas leidžia ir netgi skatina žmones pakeisti savo asmens duomenis. Tai, be jokios abejonės, taikoma kriminaliniam pasauliui. Pažinčių svetainės jau seniai pagarsėjusios didžiausiomis nuolatinėmis melagystėmis visoje istorijoje. Pokalbių svetainėse žmonės mėgsta atrodyti talentingi ir reikšmingi, nors tai retai atitinka jų kasdienio gyvenimo tikrovę. Internetas tai skatina, nes niekas negali patikrinti savo virtualių partnerių elgesio ypatumų. Visi supranta, kad internete galima meluoti, nebijant būti demaskuotam ar sugėdytam.

Nusikaltėliai ne tik vadovavosi tomis pačiomis dviveidiškumo nuostatomis, bet ir labai gerai taikė jas praktikoje. Tamsioji rinka jiems suteikė daugybę progų tai išmėginti. Pavyzdžiui, iš pokalbių registravimo žurnalų buvo galima matyti, jog šėtoniškasis Devilmanas* prisistatydavo kaip jaunas intensyvų gyvenimą gyvenantis

* *Devil* – velnias, šėtonas. (Angl.)

damų numylėtinis (nors labiausiai jis mylėjo pigias klonuotas kreditines korteles). Tačiau kai detektyvai Donkasteryje pabeldė į mažo vienbučio dviejų aukštų namelio duris adresu *62 Lime Tree Grove*, kur gyveno Devilmano *alter ego* realiame gyvenime – Johnas McHughas, juos pasitiko penkiasdešimtmetį perkopęs vyriškis, o jo pirma reakcija į žinią apie suėmimą buvo: „Ar neprieštarausite, jei pirmiausia nueisiu ir įsidėsiu dantų protezus?“ Teisme, atėjus laikui paskelbti nuosprendį, tarp kitų švelninančių aplinkybių jis paprašė įtraukti tą faktą, kad jam jau pakeistas vieno klubo sąnarys, o ir antrąjį reikia keisti, taigi jo galimybės judėti labai ribotos.

Tačiau rimti interneto nusikaltėliai, norėdami užsiimti verslu, turėjo užsitarnauti pasitikėjimą: reputacija jiems buvo svarbiausia. Tamsiojoje rinkoje Prekiautojo vardą buvo galima pelnyti tik pateikus administratoriams pirkėjų patvirtinimus, kad galite pasiūlyti rinkai tikrai veikiančias vogtas kreditines korteles. Šiuos sandėrius prižiūrėjo penki administratoriai (kai JiLsi buvo išmestas iš svetainės, o Matrica suimtas, jų liko trys – Meistras Splyntras, Štirlicas ir Cha0). Vėliau svarbus vaidmuo teko ir Lordui Cyrikui.

Cha0 įstojo į Tamsiąją rinką 2006 m. vasarį, bet puikūs sugebėjimai leido jam greitai pakilti hierarchijos laiptais. Įsitvirtinęs kaip Tamsiosios rinkos princas, jis galėjo sutelkti dėmesį į savo realaus verslo strategiją. Jis norėjo tapti pagrindiniu nelegalių kreditinių kortelių nuskaitymo prietaisų pardavėju visame pasaulyje. Šių prietaisų paklausa buvo didelė, taigi, jei jis būtų sugebėjęs sukurti monopoliją, būtų pasiekęs antrąją savo plano pakopą – mažiausiomis pastangomis kuo labiau padidinti savo pajamas.

Mūsų vyrukas iš Stambulo taip pat buvo atsakingas už pagrindinę Tamsiosios rinkos sąlyginių įsipareigojimų tarnybą, taigi, galima sakyti, turėjo pačias svarbiausias pareigas. Kaip sąžiningas tarpininkas, jis užtikrindavo, kad nei pirkėjas, nei kreditinių kortelių ir kitų nelegalių duomenų pardavėjas negalėtų apiplėšti vienas kito.

Šiuo požiūriu Tamsioji rinka tikrąja prasme buvo mafijos valdomas procesas. Ji veikė kaip kriminalinės rinkos policininkė arba arbitrė, lygiai taip kaip garbingieji Sicilijos vyrai devyniolikto amžiaus antroje pusėje pradėjo nuo žemės ūkio produktų turgų kontroliavimo, o tik paskui ėmėsi prekiauti nelegaliais ginklais ir statybų leidimais.

Cha0 savo skrupulingai sąžiningo sąlyginių įsipareigojimų tarpininko reputaciją užsitarnavo pelnęs sėkmę kaip nelegalių skaitytuvų didmenininkas. Visi juo pasitikėjo. O jis, priešingai, nepasitikėjo niekuo. Jis niekada neatskleisdavo savo IP adreso, niekada nesiųsdavo jokių žinučių, iš kurių būtų galima nuspręsti, kad jis užsiima juodais darbeliais – visada jas užšifruodavo, ir niekas jokiomis skaitmeninėmis priemonėmis negalėjo nustatyti jo buvimo vietos.

Pripažindamas, kad Cha0 internetinėje erdvėje susikūrė „juodąją skylę", Bilalas Şenas nusprendė, kad, norėdamas atsekti savo įtariamąjį, jis turės pasikliauti tradiciškesniais teisėtvarkos metodais – kaip pasitvirtino, internetinės policijos darbe sunkus triūsas turi stebėtinai svarbią reikšmę.

29
Švelniai švelniai

Stambulas, Turkija, 2008 metai

Nors ir sunerimęs, kad Cha0 gali turėti apsaugą „iš aukščiau“, Bilalas Şenas visgi atkakliai tęsė savo tyrimus. Jis pažadėjo grįžęs į Stambulą palaikyti artimus ryšius su agentu Mularskiu, esančiu Pitsburge. Juodu buvo aptarę galimybę per Tamsiąją rinką paprašyti Cha0 sąlyginių įsipareigojimų paslaugos ir pažiūrėti, gal taip pavyks jį demaskuoti, bet greitai nusprendė, kad tai reikalauja per didelių pastangų ir vargu ar duos rezultatų.

Be abejo, apie Cha0 jie žinojo ir kitką – kad jis prekiauja nelegaliais skaitytuvais. Skaitmeninėmis priemonėmis jo nebuvo įmanoma susekti. Bet jei Cha0 pardavinėja skaitytuvus, samprotavo Bilalas, tada šioje veikloje yra dvi silpnosios vietos – gamyba ir pristatymas.

Kreditinių kortelių duomenų nuskaitymas bankomatuose Turkijoje tapo toks populiarus, jog kas kartą vis daugiau policijos pareigūnų buvo mokomi pastebėti, kada nuskaitymo įrenginiai įstatomi į reikiamą vietą. Daugelis prietaisų buvo prastai padaryti ir mėgėjiškai įmontuoti. Tačiau, sklaidydamas ataskaitas apie suėmimus ir konfiskavimus, inspektorius pastebėjo, kad kai kuriose vietose skaitytuvų konstrukcija ir dizainas buvo ne tik geresnis, bet netgi atrodė, jog jie pagaminti pramoniniu būdu. Kažkur turėjo būti jų gamykla. Žvalgyba įspėjo Şeną, kad nelegalių skaitytuvų gamyklos gali būti Rumunijoje ir Bulgarijoje, taigi jis

išsiuntė pagalbos prašymus atitinkamoms tų šalių policijos tarnyboms. Kita galimybė buvo, kad Cha0, apsimetęs užsiimantis legaliu verslu, užsakinėja įrengimus iš licencijas turinčių kortelių nuskaitymo prietaisų gamintojų pačioje Turkijoje.

Gavęs skaitytuvus Cha0 vienaip ar kitaip turėjo juos paskirstyti. Mularskis ir Şenas surinko kai kuriuos įrodymus, leidžiančius daryti prielaidą, kad šie gaminiai keliauja į tokias tolimas užsienio šalis kaip Jungtinės Valstijos, Naujoji Zelandija ir Pietų Amerika ir kad kartais jie perkami dideliais kiekiais. Neatrodė, kad tokiais atvejais Cha0 naudotųsi asmeniniais kurjeriais. Atsižvelgiant į skaičius, kuriais jis pradėjo operuoti, tai būtų buvę pernelyg sudėtinga. Bilalas permąstė produktyvumo išaugimo priežastis, bet jam nepavyko ko nors nuspręsti.

Jis nežinojo, kad prieš metus, vėlyvą 2007 m. pavasarį, Cha0 susipyko su kanadiečiu nelegalių skaitytuvų specialistu Dronu, kurį Slaptoji tarnyba ir detektyvas Spenceris Frizzellis iš Kalgario policijos ruošėsi suimti. Cha0 teigė, kad Dronas buvo „sunkaus būdo“, erzino jo klientus ir kenkė Tamsiosios rinkos reputacijai. Visgi daug teigiamų atsiliepimų apie Drono paslaugas leido manyti, kad Cha0 motyvacija galėjo būti kitokia – kaip žinome, kiti karderiai iš forumo tvirtino, jog Cha0 buvo nusiteikęs prieš Droną dėl asmeninių priežasčių.

Maždaug mėnesį prieš detektyvui Frizzelliui sugaunant jauną kanadiečių kreditinių kortelių duomenų nuskaitymo ekspertą ir pardavėją, Cha0, naudodamasis einamomis administratoriaus pareigomis, paskelbė, kad Dronas bus išmestas iš Tamsiosios rinkos ir jam nebus leista grįžti. Dabar Cha0 galėjo aktyviau vykdyti savąjį dominavimo kortelių duomenų nuskaitymo rinkoje planą ir imtis konkrečių veiksmų.

Tamsioji rinka Drono gaminiams buvo suteikusi gyvybiškai svarbią platformą – daug jo prietaisų buvo parduodama karderiams, pastebėjusiems jo mokamus skelbimus forume. Tamsiąja rinka, kaip

pagrindine reklamos priemone, taip pat naudojosi ir „CrimeEnforcers.com“, per kurią savo nelegalius skaitytuvus pardavinėjo Cha0. Jis taip pat siūlė kompleksinius sprendimus, kaip tapti kibernetiniu nusikaltėliu, įskaitant mokymus, instrukcijas ir visą veiklai pradėti reikalingą įrangą.

Tačiau, pašalinęs Droną, jis pakeitė savo verslo modelį: suinteresuotos šalys nebegalėjo laisvai nusipirkti jo skaitytuvų, o turėjo juos nuomotis. Cha0 juos išsiuntinėdavo, šiek tiek pakeitęs.

Pašalinęs Droną, Cha0 galėjo smarkiai pakelti skaitytuvų kainą – nuo šiol jų nuoma kainavo 7 000 dolerių, o nusipirkti jų galima buvo už 5 000 dolerių ir daugiau. Už šią sumą klientai kartu su skaitytuvu gaudavo PIN kodo įvedimo įrenginį „PIN Pad“. Jie įmontuodavo nelegalų skaitytuvą į bankomato angą, o padirbtą „PIN Pad“ uždėdavo ant esamo įvedimo įrenginio taip, kad mygtukai sutaptų. Kai banko klientai įdėdavo korteles ir įvesdavo PIN kodus, kortelių duomenys ir PIN kodai taip pat įsirašydavo į padirbtą „PIN Pad“ ir į nelegalų kortelių skaitytuvą. Paskui abu sukčiavimo prietaisai būdavo nuimami ir Cha0 klientas perkeldavo duomenis į kompiuterį per USB jungtį.

Klientas, naudojantis Drono skaitytuvą, gavęs šią informaciją, apgaulės būdu galėdavo pats pasiimti pinigus. Bet naudojantis Cha0 skaitytuvais į kompiuterį perkelti duomenys būdavo šifruoti. O vienintelis žmogus, turintis raktą šiai informacijai iššifruoti, buvo... Cha0. Taigi pradedantysis nusikaltėlis, kuris taip uoliai dirbo, norėdamas įmontuoti nelegalų skaitytuvą ir „PIN Pad“ į bankomatą, negalėjo paprasčiausiai išeiti ir pats užsiimti kreditinių kortelių klonavimu – jam reikėjo nusiųsti informaciją atgal į Stambulą. Tada Cha0 organizuodavo grynųjų pinigų paėmimą. Turėdamas pinigus, jų dalį nusiųsdavo klientui, kuris iš tiesų buvo atlikęs visą sunkųjį darbą. Cha0 efektyviai nuomojo savo skaitytuvus – tai buvo daug pelningesnė strategija nei Drono tiesioginis pardavimas.

Kibernetinių nusikaltimų pasaulyje tai buvo bebaimis verslo modelis. Jei jis būtų sėkmingai vystęsis, Cha0 būtų galėjęs užsidirbti nesuskaičiuojamas sumas pinigų, pasisavindamas milžinišką procentą nuo nelegalių sandėrių, sudaromų visame pasaulyje, naudojantis nelegaliais skaitytuvais. Jam tereikėjo užtikrinti skaitytuvų tiekimą ir persiuntimą ir saugotis, kad jo nesusektų. Sumaniam žmogui tai visai nesunku. Aišku, galėjo ateiti laikas, kai koks nors konkurentas mėgins sužlugdyti šią strategiją ir jam iš tiesų teks grįžti prie paprasto senojo skaitytuvų pardavimo būdo. Bet kol taip atsitiks, vadovaudamas pačiam įtakingiausiam viso pasaulio anglakalbių forumui, Cha0 galėjo mėgautis prabangiu gyvenimu. Būtent tai jis ir darė.

2008 m. Stambulas pretendavo tapti sparčiausiai visame pasaulyje augančiu miestu. Gyventojų skaičius jau penkiolika metų beveik nesuvaldomai didėjo, ir dabar mieste gyveno apie penkiolika milijonų žmonių, du milijonai iš jų buvo neregistruoti migrantai, ne tik užsieniečiai, bet ir turkai bei kurdai iš Anatolijos, kurie veržėsi į miestą, išsidėsčiusį abipus didžiojo Bosforo sąsiaurio – milžiniško vandens telkinio, skiriančio Europą ir Aziją.

Priešingai nei daugelis Rytų Azijos, ypač Kinijos, miestų, Stambulas šitaip neįtikėtinai ir gaivalingai augo ne dėl patrauklaus palikimo. Tiesa, beveik kiekvienas jo pastatas mena istoriją. Visur išlikusios turtingos daugiau nei tūkstantmetės Bizantijos istorijos ir 600 metų trukusios Osmanų didybės – dviejų magiškiausių, žiauriausių, sėkmingiausių ir pagarbią baimę keliančių visų laikų imperinių struktūrų – tradicijos. Priešingai populiariai nuomonei, didumą savo istorijos Osmanų imperija garsėjo tolerancija, kurią jos valdovai rodė trijų Korane paminėtų nemusulmoniškų tikybų atstovams: žydams, krikščionims ir sabėjams*. Imperijos smurtininkės reputa-

* Sabėjai – Abraomo pasekėjų religinė grupė, tris kartus minima Korane: „Žydai, krikščionys ir sabėjai."

cija, išlikusi dėl tolimoje praeityje vykusių kruvinų skerdynių, vėl pasireiškė tik lėto jos žlugimo laikotarpiu devynioliktame amžiuje ir dvidešimto amžiaus pradžioje.

Po Pirmojo pasaulinio karo iš imperijos pelenų užgimusioje Turkijos Respublikoje Stambulas pergyveno keletą sunkių laikotarpių: pirmiausia, kai prarado šalies sostinės statusą ir šis perėjo Ankarai, iškilusiai Anatolijos regione šalies rytuose; ir vėliau, šaltojo karo metais, kai negailestingi kariškiai siekė užgniaužti nepriklausomą miesto dvasią. Jo infrastruktūra ėmė byrėti ir dalis žmonių išvyko, o gyventojų skaičius nusistovėjo ties maždaug dviejų milijonų riba. Tačiau nuo 1990 m. Stambulas pradėjo žengti pirmyn sparčiais žingsniais, siekdamas atgauti savo svarbią vietą tarp dinamiškiausiai besivystančių ir įdomiausių pasaulio miestų.

Tankiai apgyventas, triukšmingas ir sparčiai besivystantis, vykstant ekonominiams mainams tarp jo Europos ir Azijos sektorių, ir su dešimtimis tūkstančių išklibusių automobilių ir sunkvežimių, kursuojančių dviem jo tarpžemyniniais tiltais, Stambulas kartais atrodo troškus. Europinėje pusėje transportas sraigės greičiu juda aplink Taksimo aikštę arba Dolmabachčės gatve pro buvusius imperijos sodus, atsigręžusius į Azijos pusę. Dulkės skverbiasi giliai į gerklę, net kai oras vėsus. Bet per paskutinį dešimtmetį mieste atsivėrė begalė įvairiausių galimybių meno, verslo ir politikos srityse, o ir šiaip gyvenime ne taip dažnai pasitaiko malonumų, kai po sunkios darbo dienos gali sėsti į keltą Europoje, pasižvalgyti po Bosforo sąsiaurį ir, persikėlęs į Azijos pusę, pasilepinti puikiais valgiais Stambulo Kedikejaus rajone.

Nepaisant nuogąstavimų, kad į valdžią atėjusi AK partija gali tapti islamiškojo fundamentalizmo penktąja kolona, jauna Stambulo vidurinė klasė visomis išgalėmis griebėsi ekonominių galimybių ir pradėjo kurti sėkmingai besiverčiančias apdirbimo, dizaino, moderniųjų technologijų ir paslaugų kompanijas, kurios konkuruoja su geriausiomis savo srities atstovėmis iš Europos, Amerikos ir Azijos.

Žinoma, palaikyti teisėtvarką mieste košmariškai sunku, ypač todėl, kad labai mažai gyventojų bent kiek pasitiki pajėgomis, kurios daugelį metų buvo pagrindinis represinio valstybės aparato simbolis.

Nauji nusikaltimai pagimdė naują policininkų rūšį, o Bilalas nebuvo susijęs su jokiomis senomis „valstybės valstybėje" tradicijomis. Antra vertus, priešų tarp galingųjų jis taip pat neturėjo. Taigi jis buvo šiltai sutiktas Stambule, kai atvyko iš Turkijos sostinės Ankaros atskleisti Cha0 kreditinių kortelių duomenų nuskaitymo prietaisų platinimo tinklo.

Visgi tokiame mieste kaip Stambulas inspektorius Şenas ieškojo adatos šieno kupetoje. Legalus, pusiau legalus ir nelegalus eksportas ir importas šimtmečiais buvo miesto ekonomikos skiriamasis požymis – prekės judėjo iš miesto ir buvo įvežamos į jį. Nuo praeito amžiaus septintojo dešimtmečio milžiniški kiekiai buitinių prekių per Balkanus buvo įvežami iš Vokietijos, į kurią septintajame dešimtmetyje persikėlė apie du milijonus darbo užsienyje ieškančių turkų. Tačiau šios prekybos mastai dar greičiau išaugo subyrėjus Sovietų Sąjungai: naujos rinkos atsivėrė Rusijoje, Ukrainoje, Kaukaze ir keliose Centrinės Azijos respublikose, kuriose kalbama tiurkų kalbomis.

Bet Bilalui reikėjo kažkaip pradėti, taigi jis pasirinko tris didžiausias prekių gabenimo įmones mieste. Pirmiausia jis ir jo asistentai pusę dienos praleido mokydami vežėjų kompanijų personalą atpažinti nelegalius skaitytuvus. Dažniausiai jie įregistruojami kaip automobilių ar prietaisų atsarginės dalys. Personalui buvo leista skaitytuvus apčiupinėti, kad įsidėmėtų jų svorį ir formą.

Tuščiai prabėgo ne viena diena, ir inspektorius Şenas nusprendė grįžti į centrinę būstinę Ankaroje. Praėjo savaitė, ir jį apėmė jau pažįstamas nusiminimas. Tačiau tada, kiek daugiau nei po mėnesio, iš Stambulo atskriejo gera žinia – į vieną vežėjų kompaniją atėjo vy-

riškis, nešinas paketu, kuris turėjo būti nugabentas į Suomiją. Išaiškėjo, kad pakete buvo nelegalus skaitytuvas. Sekretorius skambino iš nuošalaus kabineto, kad praneštų naujieną, jog pakete taip pat yra ir „PIN Pad".

„Puiku!" – pamanė Bilalas ir liepė sekretoriui paleisti siuntėją: su uždaros televizinės sistemos kamera jie jau buvo užfiksavę jo atvaizdą. Po daugelio mėnesių inspektoriui pagaliau pasisekė. Nenuostabu, kad vyriškis naudojosi padirbta asmens tapatybės kortele, tačiau tada Bilalui pasisekė antrą kartą. Įtariamasis vežėjų kompanijai taip pat įteikė tris telefono numerius, iš kurių vienas buvo tikras. Jie patikrino pavardę, norėdami išsiaiškinti telefono savininką. Neatrodė, kad telefonas priklausytų nusikaltėliui. Bet jie patikrino ir mobiliojo telefono numerį, kuriuo naudojosi vyriškis, atnešęs paketą, – telefonas veikė.

„Tai gali būti vaikinas, kuris atves mus prie Cha0", – pagalvojo Bilalas.

Tačiau jis susidūrė su dilema. Maždaug tuo pat laiku naujienų agentūra „Haber 7" išspausdino pažeminto programišiaus Merto Ortaço nuotrauką, taigi tiek Stambulo policija, kuriai buvo duota užduotis surasti Ortaçą, tiek ir Bilalas, kurio pagrindinis taikinys buvo Cha0, buvo smarkiai spaudžiami. Bilalui reikėjo greitinti įvykių eigą, bet jis suprato, kad turi neprarasti kantrybės, nes kitaip gali pastatyti į pavojų visą operaciją.

Panaudojęs prievartą prieš Ortaçą, Cha0 pirmą kartą išdavė savo nerimą ir pažeidžiamumą. Bet kodėl Ortaço pareiškimai per „Haber 7" jį taip sutrikdė?

Cha0 žinojo, kad Ortaças yra turkas. Be to, atrodė, jog Cha0 mano, kad Ortaças yra policijos informatorius. Dar daugiau, jis išsiaiškino, kad Ortaças slapstosi ir yra įsibaiminęs. Jei policija pagautų jį anksčiau nei Cha0, kiltų grėsmė, kad jis gali prasitarti.

Tačiau kas, po galais, yra tas Mertas Ortaças ir kaip jis buvo įtrauktas į šią neeilinę nusikalstamą aferą? Viskas prasidėjo praeitą pavasarį, kai, nežinant Ortaçui, buvo ruošiamasi suimti Matricą ir JiLsi ir taip pažymėti operacijos „DarkMarket“ pirmosios stadijos pabaigą ir antrosios pradžią.

III dalis

Per metus Tamsioji rinka nuvedė mane toli nuo „Google" pagrindinės būstinės – į „Cihangir" restoraną prabangiame rajone europinėje Stambulo dalyje, šiek tiek į pietus nuo *Taksim* aikštės. Žvelgiau į spindinčią Merto Ortaço šypseną. Praleidęs kelias valandas jo draugijoje, aš padariau išvadą, kad būdvardis „piktdžiugiškas" niekada niekam šioje žemėje netiko taip gerai kaip Mertui.

Per vieną tingią vakarienę Kedikejaus rajone mano draugo Şebnemo ir mano išmanieji telefonai gulėjo ant stalo. Staiga jie abu pyptelėjo – tuo pat metu mudu gavome tekstines žinutes. Mano gautoji žinutė buvo išsiųsta iš Şebnemo telefono, o Şebnemo – iš manojo. Abiejose buvo parašyta: „Sveikinimai nuo Merto!" Mums beskaitant žinutes, kitapus stalo sėdintis Mertas pratrūko linksmai juoktis ir paaiškino, kad jam pavyko sėkmingai įsilaužti į tarptautinę tarptinklinio ryšio sistemą. Todėl, aiškino jis, jis galįs išsiųsti žinutę iš bet kurio mobiliojo telefono pasaulyje į bet kurį kitą. Piktam naudojami (kaip Merto atveju) tokie gebėjimai gali paversti žmogaus gyvenimą nesibaigiančiu serialu su Shakespeare'o plunksnos vertu siužetu, pilnu tiek tragiškų, tiek komiškų nesusipratimų.

Aš susirašinėjau su Mertu, kol jis sėdėjo kalėjime, iš kur siųsdavo man trumpus pasakojimus, išradingumu pralenkiančius visas kitas legendas apie Tamsiąją rinką. Kalbėdamas su daugeliu kitų veikėjų, susijusių su Tamsiąja rinka, buvau tikras, jog jie nuslepia kai kuriuos dalykus, o Mertas mane tiesiog užtvindydavo informacija, anekdotais ir sunkiai įsivaizduojamomis istorijomis.

Programišiams, kibernetiniams nusikaltėliams ir kibernetinei policijai labai svarbu valdyti savo iš atskirų segmentų susidedantį gyvenimą – jie turi jausti ribas, skiriančias realų pasaulį nuo virtualaus, ir turi sugebėti atsiriboti, pereidami iš vieno savo gyvenimo į kitą. Tačiau Mertas visiškai nepajėgė valdyti savo minčių ir pats neskyrė, kada kalba tiesą, o kada meluoja.

Gyvenimas būtų buvęs nepalyginti lengvesnis, jei Mertas būtų buvęs gėdos nejaučiantis fantazuotojas, paprasčiausiai tauškiantis nesąmones. Programišių, Tamsiosios rinkos narių ir su ja susijusių policininkų sekimas buvo viena iš labiausiai alinančių mano žurnalistinės karjeros patirčių. Bet niekas nebuvo taip nepakenčiama kaip pastangos nustatyti Merto istorijų tikrumą. Iš tiesų ne visai tiksliai pasakyta: paaiškėjo, kad didelė jo pasakojimų dalis iš esmės buvo tiesa, kurią buvo galima įrodyti, bet kartais pasakojimai būdavo pagražinami tokiomis įmantrybėmis ir vingrybėmis, kad visai pasikeisdavo. Keista, bet kai Mertas sakydavo visišką netiesą, tai dažnai būdavo susiję su žemiškiausiais dalykais, kuriuos būdavo lengviausia patikrinti. Pavyzdžiui, sykį jis išdidžiai man pranešė, kad yra gimęs 1982 m. balandžio 10 d. Iš tiesų jis gimė tą dieną, tik po ketverių metų.

Tolesniuose skyriuose aš pasakoju Merto istoriją didžia dalimi taip, kaip jis pats man ją papasakojo. Tačiau yra du esminiai momentai, kai jo pasakojimas yra nenuoseklus, ir aš negaliu patvirtinti jo teiginių; iš tikrųjų pirmu atveju vienas iš pagrindinių veikėjų kategoriškai neigia Merto įvykių versiją. Aš įspėsiu skaitytoją, kai priartėsime prie šių momentų.

Pagrindinis Merto patikimumo patikrinimas susijęs su jo atsakymu į klausimą, nuo pat Tamsiosios rinkos atsiradimo kėlusį daug ginčų tarp daugelio kibernetinio pogrindžio entuziastų. Kas tas Lordas Cyrikas?

30
Merto Ortaço fantazijų pasaulis

Stambulas, Turkija, 2007 m. gegužė

Mertas Ortaças sulaikė kvapą, kai jį įvedė į prabangių svečių namų svetainę. Kambarys jam priminė prašmatnius sultono apartamentus *Çirağan* rūmuose, devyniolikto amžiaus pabaigos šedevre, kuris buvo pastatytas jo imperatoriškosios didenybės sultono Abdülazizo įsakymu ir kurį visai neseniai įsigijo Kempinskio viešbučių tinklas. Auksinių lapų apvadai puošė sofas ir kėdes, o sienų apmušalai su arabiškais raštais žėrėjo saulės šviesoje.

Iš tiesų *Çirağan* rūmai stovėjo tik už 800 jardų nuo svečių namų, kuriuos supo akylai saugoma uždara teritorija. Apsaugos darbuotojai išdidžiai žingsniavo aplinkui ir rūsčiai nužvelgdavo kiekvieną, beatodairiškai mėginantį pasistatyti čia savo automobilį. Didžiulis namas, esantis pačiame Bešiktašo rajono pakraštyje, nuo kalvos viršaus Europos pusėje per Bosforo sąsiaurį išdidžiai žvelgė į Aziją. Labiausiai stebino tai, kad svetainėje, į kurią atvedė Mertą, nebuvo garbinamo šiuolaikinės Turkijos įkūrėjo Kemalio Atatürko portreto. Kemalio portretai privalomi visoje Turkijoje, ir ne tik privačiuose biuruose ir visuomeninėse įstaigose: dažnai juos rasite kiekviename pastato kambaryje. Bet ne šiame kambaryje, nors tai buvo Turkijos nacionalinės žvalgybos agentūros MİT (turk. *Milli İstihbarat Teşkilati*) Stambulo regioninės būstinės svečių kambarys.

Patekęs į nerimą keliančias situacijas Mertas dažniausiai arba negarsiai kikendavo, dangstydavosi piktdžiugiška šypsena, arba bailiai pasišalindavo. Šiuo atveju nė vienas variantas netiko. Arbatą ir kavą pateikusių elegantiškų padavėjų akivaizdoje Mertas jautėsi susikaustęs. Be viso kito, jo atmintyje išliko jų baltutėlaičių pirštinių vaizdas, kai ant stalo priešais jį dėliojo užkandžius ir gaiviuosius gėrimus. Jį užvaldė netikroviškas gerovės ir saikingo jaudulio pojūtis. Bet tai truko neilgai.

Jį lydėjo kolega iš Aukštesniojo mokslo ir technologijų instituto, bet Mertas nepažinojo kitų trijų, pasisveikinusių su juo. Kai tik padavėjai tyliai pasišalino, šie vyrai sutelkė dėmesį į Mertą. „Norime užduoti jums keletą klausimų", – pradėjo vienas iš jų. Tada priešais jį ant stalo jie padėjo skaitmeninį diktofoną.

Visai neseniai jis liejo prakaitą per įtemptą apklausą. Bet tai nebuvo kvota. Ne, šešias su puse valandos Mertas turėjo spręsti aibę velnioniškai sudėtingų matematikos uždavinių. Normaliomis aplinkybės jis net nebūtų mėginęs jų išspręsti be kompiuterio. Trys angelai sargai paprašė jo išskaidyti skaičių penkiasdešimt du į nelyginius skaičius, pritaikius populiarią metodiką, naudojamą koduojant. Tai buvo labai pažangi matematika, o jis turėjo tik rašiklį ir lapą popieriaus.

Jaunas kompiuterių programuotojas jau buvo neišlaikęs atrankinio egzamino, kuris būtų leidęs pripažinti jį tinkamu tapti bandomuoju Žvalgybos agentūros darbuotoju. Jis išlaikė užsienio kalbos (anglų) testą ir matematiką, bet siaubingai susimovė per turkų kalbos egzaminą. Vis dėlto agentūra buvo susižavėjusi jo kompiuteriniais įgūdžiais. Jo gabumai programuoti buvo tikrai neeiliniai ir jis turėjo labai gerą charakteristiką, taigi jie priėmė jį laisvai samdomu darbuotoju.

Dar 2003 m. dėl sukčiavimo Mertas buvo tapęs kriminalinių tyrimų objektu. Vos septyniolikos jam pavyko išsiaiškinti lustinių

kortelių*, kuriomis naudojosi palydovinės televizijos stotis „Digiturk“, šifravimo kodą. Šis gebėjimas atnešė pelno. „Digiturk“ neseniai buvo laimėjusi teisę transliuoti „Super Lig“ (labai populiarias aukščiausio lygio Turkijos futbolo varžybas). Norėdami atkoduoti kanalą, abonentai turėjo iš „Digiturk“ nusipirkti lustinę kortelę ir įkišti ją į palydovinį imtuvą, tik tada būdavo įleidžiami į futbolo rojų.

Kai Mertui pavyko įsilaužti į šias korteles, jis ėmėsi jas atgaminti, kad galėtų nelegaliai pardavinėti Stambulo gatvėse, ir šitaip užsidirbo daug pinigų. Kai tik kišenė prisipildydavo turkiškų lirų, jos tuojau pat išbyrėdavo. Mertas rengdavo vakarėlius draugams iš Ankaros, apmokėdavo jų kelionių ir pragyvenimo išlaidas, kai jie pasiekdavo Stambulą. Jis niekada negebėjo kontroliuoti savo išlaidų, net ir vėliau, kai iš kardingo veiklos gaudavo solidžias pajamas.

Draugai Mertui buvo labai svarbūs, iš dalies todėl, kad jam ne visada sekėsi meilės reikalai. Nežinia, ar jis pats tai suprato, ar ne, bet iš „Digiturk“ uždirbtus pinigus jis naudojo draugystei pirkti – o Stambule buvo pilna kiek vyresnių nei dvidešimties metų jaunuolių, pasiruošusių bičiuliautis su jaunu vaikinu, rodančiu aiškų norą sumokėti už brangius vakarėlius. Be abejo, kai pinigai pasibaigdavo, dauguma šių veikėjų paprasčiausiai dingdavo.

Mertas taip pat desperatiškai troško įrodyti esąs neeilinis vaikinas (vertinant jo talentą kompiuterių srityje, toks jis neabejotinai ir buvo). Taigi jis amžinai perdėdavo savo laimėjimus. Stiprėjant šiai tendencijai, Merto sąmonė ėmė nuolatos klajoti tarp tikrovės ir fantazijų. Atrodė, kad jau ankstyvoje šios sumaišties stadijoje jis prarado gebėjimą atskirti vieną nuo kito. Jis buvo taip susipainiojęs, kad jei

* Lustinė kortelė – mokėjimo kortelė su įdiegtu lustu (mikroprocesoriumi), kuriame yra saugomi duomenys apie kortelės savininką. Pagaminti tokios kortelės dublikatą yra sunkiau nei įprastos magnetinės kortelės, todėl jos laikomos saugesnėmis.

kada nors jam būtų tekę atlikti testą melo detektoriumi, prietaisas, ko gero, būtų arba išėjęs už skalės ribų, arba nebūtų užregistravęs nė vieno signalo. Žinoma, tai savotiškai rodė, kad jis lengvai prisitaikė prie interneto – melo slėnio – kultūros.

Po daugybės darbų, atliktų informacinių technologijų srityje įvairioms kompanijoms, 2006 m. birželį Mertą priėmė į darbą vietinis „Toshibos" filialas, kurio personalo skyrius nepastebėjo, kad vyro vardas siejamas su kriminaliniu tyrimu dėl sukčiavimo „Digiturk" byloje. Vis dėlto neilgai trukus Merto kolegas iš „Toshibos" kompanijos pradėjo stebinti jo elgesys. Įtartinas jiems pasirodė ir pažymėjimas, įrodantis, kad jis turi Kembridžo universiteto kriptologijos mokslų mokslinį laipsnį.

Universiteto globėjai, buvo rašoma pažymėjime, „suteikė šį diplomą kaip atitinkamą įrodymą, išduotą Londono mieste, Kembridže, du tūkstančiai ketvirtų metų birželio dvidešimt antrą dieną".

Galbūt jie išdavė diplomą „Cambridge Arms" alinėje, esančioje Londono mieste? Kad ir kur būtų įvykusi ši fiktyvi ceremonija, pažymėjimas buvo sukurptas taip negrabiai, jog net klastote jį vargu ar galėjai pavadinti.

Vieną kolegą iš „Toshibos" Informacinių technologijų skyriaus priblokšė tai, kad Mertas labai dažnai gyrėsi savo santykiais su Nacionaline žvalgyba. Tasai kolega seniau taip pat kartkartėmis siūlydavo pagalbą šnipams, ypač praeito amžiaus paskutinio dešimtmečio pabaigoje, kai Žvalgybos agentūra dar tik kūrė veiksmingą kibernetinį padalinį. Bet jis nesigyrė tokiais dalykais. Nuolatinis Merto burbėjimas apie artimus santykius su žvalgyba tikrai rėžė ausį. „Toshiba" jį laikė šešis mėnesius, nes kas kartą viršininkams paprašius išspręsti kokią nors problemą, Mertas visada pateisindavo jų lūkesčius. Jie laikė jį labai sumaniu, bet kažkas tarsi perspėjo juos nenuleisti nuo jo akių.

Vakare Mertą išsikviesdavo jo vadai iš Žvalgybos agentūros ir prašydavo įvertinti įvairiuose standžiuosiuose diskuose ir kompiuteriuose esančius įkalčius, kuriuos jie, atrodo, traukdavo nežinia iš kur. Visomis įmanomomis priemonėmis jis turėdavo „išmėsinėti" failus, įsilaužti į slaptažodžius ir pateikti kokią nors kaltinamąją medžiagą. Pagrindinė agentūros užduotis buvo atsakomybė už Turkijos vidaus saugumą, ir ji privalėjo kontroliuoti platų spektrą organizacijų, kurios, vyriausybės nuomone, buvo susijusios su terorizmu.

2006 metams artėjant į pabaigą, „Toshiba" atleido Mertą – dėl netinkamo požiūrio į darbą ir dėl to, kad jis per daug mėgo girtis savo abejotinais žygdarbiais su kreditinėmis kortelėmis, nors vis tiek amžinai prašinėdavo kolegų paskolinti pinigų ar už ką nors jam papildomai sumokėti.

Mertas tvirtino, kad išėjo iš „Toshibos", palieptas savo vadovų iš Nacionalinės žvalgybos agentūros. Jis sakė, kad jie ieško jam kito darbo.

Prieš pat įsidarbinant naujoje tarnyboje, jo vadovas atnešė jam standųjį diską, kuris buvo susijęs su labai svarbiu tyrimu. Valdžia norėjo viską žinoti apie kiekvieną failą, įrašytą į diską, nesvarbu, ar jis būtų matomas, ar paslėptas, prieinamas ar užšifruotas. Diskas priklausė vienam iš kairiosios pakraipos pogrindinės organizacijos „Revoliucinė liaudies išlaisvinimo armija / frontas / partija", žinomos sutrumpintu pavadinimu DHKP-C, vyresniųjų narių.

Per praeito amžiaus paskutinį dešimtmetį ir šio amžiaus pirmojo dešimtmečio pradžioje DHKP-C buvo viena iš įnirtingiausių ir veiksmingiausių ginkluotai kovai pasiruošusių Turkijos kairiosios pakraipos organizacijų. „Revoliucinė liaudies išlaisvinimo armija / frontas / partija" (partija buvo politinis sparnas, o frontas – karinis sparnas) – tai grupė, atskilusi nuo dar didesnio revoliucinio judėjimo „Dev Sol", atlaikiusio pagrindinius karinių represijų smūgius praeito amžiaus aštuntajame ir devintajame dešimtmečiuose.

Tai nebuvo kukli frakcija – savo politiką ir terorizmą ji vertino rimtai ir svarbiausią dėmesį skyrė atakoms, nukreiptoms prieš tai, ką ji skelbė esant NATO imperializmo ir Turkijos karinių pajėgų kolaboravimu. Ji įvykdė sėkmingus teroro aktus prieš turkų, amerikiečių ir britų tautybių gyventojus, kurie buvo arba įtakingi verslininkai, arba susiję su kariškiais. Kitaip nei dauguma ginkluotų kairiųjų grupių, ji didžiavosi moderniomis kovos su žvalgyba priemonėmis ir dėl to tapo vienu iš sudėtingiausių Nacionalinės žvalgybos sekimo objektų.

Per vieną reidą agentai konfiskavo nešiojamąjį kompiuterį ir perdavė jį Mertui svečių namuose, kur pirmą kartą buvo su juo kalbėta ir kur dabar jis nuolatos dirbo. Jo vadovas paaiškino, kad kompiuterio naudotojas turėjo prieigą prie svetainės, vadinamos „DarkMarket". Vadovas taip pat buvo kompiuterių entuziastas ir pasisakė Mertui atsekęs Tamsiosios rinkos ryšius iki pat serverio, esančio Singapūre, ir šis jam pasirodė panašus į įgaliotąjį serverį. Paskui, anot jo, jis pametė skaitmeninį pėdsaką. Jis nieko nežinojo apie tai, kas slepiasi už šios svetainės, nors įrodymai aiškiai bylojo, kad DHKP-C užsiima kardingu kaip būdu savo pajamoms padidinti, ir gali būti, jog taip pat tyrinėja kenkėjiškomis programomis užkrėstų kompiuterių tinklų naudojimo galimybę, mėgindama išsiaiškinti, ar tai gali padėti DHKP-C siekti savo tikslų.

Netikėtai „DarkMarket" tapo ne vien kriminaline svetaine: ji padėjo finansuoti minėtą teroristinę organizaciją.

Vadovas paklausė, ar Mertas ką nors žino apie šią svetainę.

Ne, Mertas nežinojo. Jis taip pat atsekė Tamsiosios rinkos serverį iki Singapūro, bet, kad ir kiek stengėsi, nieko daugiau atsekti nevaliojo. Iš tiesų taip nutiko dėl rimtų Grendelio pastangų. Tačiau Mertas savo vadovui pasakė žinąs vieną žmogų, kuris gali būti geriau susipažinęs su Tamsiąja rinka.

Mertas buvo pavargęs. Nacionalinė žvalgyba, kaip visada, tikėjosi, jog jis atliks šį darbą per naktį. Jo nauja darbovietė buvo Turkijos „Fox" televizijos koncesija. Turkijos „Fox" nevisiškai priklausė Ruperto Murdocho „News International" kompanijai, kadangi, vadovaujantis Turkijos įstatymais, 51 procentą akcijų turėjo valdyti vietinis gyventojas. Šis pagrindinis akcininkas – buvęs diplomatas, kuris, aišku, turėjo ryšių su policija ir slaptąja tarnyba. O Merto kolegos iš „Fox" televizijos pastebėjo, kad jis dažnai, jei ne visuomet, yra išsiblaškęs. Ir kad jam sunkiai sekasi iki galo padaryti net ir paprastus darbus – ne todėl, kad nesugebėtų jų atlikti, bet todėl, kad tuo pat metu jis užsiėmęs kažkuo kitu.

Vienas Merto bičiulis, su kuriuo jis palaikė ryšį, buvo prašęs jaunuolį atidžiai stebėti kažkokį Saduną Özkayą, paauglį iš vidurinės klasės, kurio tėvai buvo susirūpinę, jog jų atžala susipainiojo gyvenime. Vaikis ką tik buvo ištrauktas iš kalėjimo ir prieš jį buvo atliekamas tyrimas dėl sukčiavimo. Bičiulis prašė Merto dorai elgtis su Sadunu – o tai buvo tas pats, kas įkalbinėti vilką aiškinti vegetarizmo naudą kitam vilkui, kai tuo pat metu jie abu laižosi snukius, palinkę prie jauno ir minkšto ėriuko likučių.

Mertas nutuokė apie kriptografiją ir programavimą; Sadunas nutuokė apie kreditines korteles. Netrukus juodu sujungė savo įgūdžius. Ir, didelei Merto nuostabai, Sadunas jam prisipažino esąs Tamsiosios rinkos narys ir kad lankosi joje, naudodamasis dviem slaptažodžiais: Cryptos ir PilotM. Nepraėjus nė valandai, Mertas Ortaças jau registravosi pastaruoju slapyvardžiu.

„O stebukle!" – pamanė Mertas, pirmą kartą patekęs Tamsiosios rinkos vidun:

Kiek čia žavių būtybių!
Kokia puiki vyrija! Koks puikus naujas pasaulis,
kuriame yra tokių žmonių!

Mertas neteko žado. Jis ištyrinėjo kiekvieną svetainės kampelį ir plyšelį, pasižvalgė po forumus, mokydamasis imituoti jos narių žargoną, o paskui pamėgino atskleisti jos paslaptis kiek suktesniais metodais. Iki šiol Merto kriminaliniai siekiai buvo įsilaužti į lustines korteles, iššifruoti jų kodavimo sistemas ir parduoti klonuotas korteles. Išlaisvinęs savo vaizduotę Tamsiojoje rinkoje, jis greitai įsisavino naujus patarimus, kaip sukčiauti su kreditinėmis kortelėmis. Šių įgūdžių derinys jį ir Saduną atplukdė į labai drumstus, nors finansiškai ir naudingus vandenis.

Tačiau prieš tai jis pradėjo smulkiai analizuoti Tamsiąją rinką, tarsi tai būtų pogrindiniai pinklių pilni labirintai su paslėptais lobiais. Jo vadai iš Nacionalinės žvalgybos, be abejo, norėjo sužinoti viską, kas buvo susiję su jų tyrinėjama teroristine organizacija DHKP-C. Tačiau Mertas labiau domėjosi visais kitais dalykais, kurie dėjosi forumuose.

Labai greitai jis suprato, kad Cha0, Meistras Splyntras ir Lordas Cyrikas yra pagrindiniai svetainės veikėjai. Mertui pradėjus reikštis Tamsiojoje rinkoje, JiLsi ir Matrica jau buvo iš jos pašalinti.

Jam prireikė vos kelių sekundžių išsiaiškinti, jog Cha0 yra turkas, nors tai atsitiko visiškai atsitiktinai ir niekaip nebuvo susiję su jo, kaip įsilaužėlio, sugebėjimais. Jis paprasčiausiai naršė po Cha0 nelegalių skaitytuvų reklamas ir fone pastebėjo turkišką „Doner" kebabų ženklą. Kitoje nuotraukoje parduodamas skaitytuvas buvo padėtas greta turkiškų skalbimo miltelių.

Žinia apie didelę turkų įtaką internete jis pasidalijo su savo vadovu iš Žvalgybos agentūros, ir šis dar labiau susidomėjo Tamsiąja rinka: pasirodo, svetainėje ne tik aktyviai reiškėsi kairiųjų pažiūrų teroristai, bet jai iš tiesų vadovavo turkai! Tai galėjo būti kažkas labai svarbaus, taigi reikalavo tolesnių tyrimų. Mertui buvo suteiktas įgaliojimas susisiekti su Cha0 ir kitais turkais, kuriuos jis rado

besibūriuojančius aplink Tamsiosios rinkos forumą. Netrukus jam pasirodė, jog atpažino dar vieną – Lordą Cyriką.

Mertas pradėjo tyrinėti praeito amžiaus paskutinio dešimtmečio archyvus, kai daugelis kompiuterių entuziastų naudojosi vadinamąja skelbimų lentos paslauga, sutrumpintai BBS (angl. *Bulletin Board Service*), kuri buvo savotiškas tiltas tarp elektroninės keitimosi žinutėmis sistemos ir interneto. Žiūrinėjant pokalbių registravimo žurnalus, jam atvipo žandikaulis, greta vienas kito užtikus du pažįstamus slapyvardžius: Cha0 ir Lordo Cyriko! Ko gero, nusprendė jis, šiuodu pagrindiniai Tamsiosios rinkos protai jau seniai pažįsta vienas kitą.

31
Dviejų ponų tarnas

Pramanytas veikėjas Lordas Cyrikas tarp kompiuterių ir kompiuterinių žaidimų fanatikų tapo populiarus praeito amžiaus devintajame ir dešimtajame dešimtmečiuose. Pasiskelbęs dievybe, jis klaidžiojo po Užmirštas karalystes – Dievo apleistą išgalvotą pasaulį, kuriame bastėsi kariai, ieškantys lobių ir tamsių paslapčių ir kariaujantys su magiškų galių ir pragaištingų tikslų turinčiomis būtybėmis. Karalystės tapdavo kompiuterinių žaidimų entuziastų mėgstama tyrinėjimų teritorija, kai jie, prisiėmę išgalvotus vaidmenis nuotykių ieškotojų komandoje, žaisdavo žaidimą „Požeminiai kalėjimai ir drakonai". Vėliau šios nederlingos žemės, panašios į Tolkieno vaizduotą pasaulį, pasirodė daugelyje kompiuterinių žaidimų, tarp jų ir labai didelio populiarumo sulaukusiame žaidime „Balduro vartai".

Tos karalystės taip pat buvo aprašytos daugelyje romanų, kuriuos įkvėpė tiek „Požeminiai kalėjimai ir drakonai", tiek *Žiedų valdovas*. Užmirštų karalysčių mitologijoje labai svarbų vaidmenį vaidino Lordas Cyrikas – būdamas dievas, tuo pat metu jis buvo tikras velnias. Kalbant apie kardingo ir Tamsiosios rinkos pasaulius, dar svarbiau yra tai, jog Cyrikas, be kita ko, buvo Melo princas, turintis šėtoniškų galių meistriškai sukčiauti ir apgaudinėti, taip pat gebąs kelti vaidus ir intrigas.

Kad ir kas buvo tas veikėjas, kuris slėpėsi už avataro Karderių rinkoje, Tamsiojoje rinkoje ar kur kitur, jis norėjo sukurti tai, ką „Požeminių kalėjimų ir drakonų" žaidėjai vadino „chaotišku blogiu",

tuo norėdami pasakyti, jog kad ir kur šis veikėjas klajotų, jis tarsi atsitiktinai barstė sąmyšio ir nevilties sėklas. Lordui Cyrikui iš Tamsiosios rinkos neabejotinai labai tiko toks apibūdinimas dėl jo polinkio į suktybes, apgavystes, vaidus ir intrigas. Nedaug karderių buvo sukėlę tiek priešiškumo bendruomenėje, kiek šis veikėjas. Jis pasižymėjo sugebėjimu skleisti kaltinimus per gandus ir užuominas.

Dėl nesuprantamų priežasčių Cyrikas pasirinkdavo tam tikrą objektą, tarkim, Raudonąją Brigadą, kuris Niujorke taip pelningai naudojosi „Shadowcrew". Tada tūkstančiais smūgių mėgindavo sugriauti jo reputaciją tarp karderių. Nedidelė užuomina ar nedidelis šmeižtas šen bei ten apie tai, jog Raudonoji Brigada yra visai ne toks, koks atrodo, arba užkoduoti pareiškimai, teigiantys, jog Raudonoji Brigada iš tiesų dirba teisės ir teisėtvarkos institucijoms. Cyriko kalba buvo paini ir vaikiška, bet rūpestingai apgalvota, kad maksimaliai pakenktų jo atakų objektui.

Vis dėlto ir šioje srityje Cyrikas turėjo varžovų – pats stipriausias iš jų buvo Cha0. Su savo neeiliniu protu ir atitinkamu pranašumo kompleksu Cha0 pripažino sau lygiais iš viso tik du kompiuterininkus. Jo panieka FTB kibernetinių nusikaltimų padaliniui buvo beribė, bet jis nuoširdžiai pripažino Makso Vizijos (vėliau pasivadinusio Ledo Žmogumi) sugebėjimus įsilaužti, nors su Cyriku juodu kartais smarkiai kivirčydavosi dėl Ledo Žmogaus atakų, nukreiptų prieš Tamsiąją rinką. O kalbant apie Lordą Cyriką, Cha0 buvo nuėjęs taip toli, kad savo seną draugą beveik pripažino programišių panteone iškilusiu netgi aukščiau už save patį.

Per trumpą laiką Lordui Cyrikui pavyko tapti pagrindiniu moderatoriumi ir administratoriumi tokiuose forumuose kaip „The Grifters"*, „CardersMarket" ir galiausiai „DarkMarket". Niekas nesuprato, kokį žaidimą jis žaidžia ar ką nori pasiekti, nors

* Sukčiai. (Angl.)

tie, į kuriuos jis nusitaikydavo, iš karto imdavo manyti, kad jis dirba teisėsaugai kaip pareigūnas arba kaip konfidencialus informatorius.

FTB agentas Keithas Mularskis iš Pitsburgo nė nenutuokė, kas tas Lordas Cyrikas. Kaip ir daugelis kitų, jis tikėjo, kad žmogus slapyvardžiu Lordas Cyrikas gyvena Monrealyje, Kanadoje, bet jo užklausimai Kanados karališkosios raitosios policijos RCMP (angl. *Royal Canadian Mounted Police*) kibernetinių nusikaltimų padaliniui nesukėlė jam jokio džiaugsmo. Iš tiesų, nors Cyriko IP adresus buvo galima atsekti iki Monrealio, kartais jie pasirodydavo esą Toronte, kur, kaip įtarė kai kurie sekliai, jis iš tiesų gyveno.

Keli karderiai pasigavo ir paskleidė gandą, kad Lordas Cyrikas iš tiesų yra Brianas Krebsas, žurnalistas, kuris tuo metu dirbo laikraštyje *The Washington Post* ir rašė apie kibernetinį saugumą. Nebuvo jokių tai patvirtinančių įrodymų – iš tikrųjų netgi priešingai, nes Krebsas buvo per daug rimtas rašytojas, kad rizikuotų sugriauti savo reputaciją, susidėdamas su tais žmonėmis, kuriuos pats tyrinėjo. Vėliau sklandė daugybė gandų, bet niekas niekada taip ir nepriartėjo prie atsakymo į klausimą, kas iš teisybės buvo Lordas Cyrikas ir ką jis veikė.

Skatindamas kitus įsitraukti į visų rūšių įtartiną veiklą, Lordas Cyrikas pats niekada neužsiimdavo kriminaliniais sandėriais, o tai tik sustiprino įspūdį, kad jis dirba kokiai nors teisėsaugos ar žvalgybos institucijai.

Tačiau visi tikėjo, kad Lordas Cyrikas daug žino apie kardingo bendruomenę ir apie tai, kaip ji veikia. Štai kodėl jis buvo labai populiarus ir reikalingas. Karderiai norėjo, kad jis suvestų juos su bendraminčiais, už kuriuos jis galėtų garantuoti, arba norėjo žinoti, ką jis mano apie vieną ar kitą veikėją. O JAV ir Vakarų Europos policijos tebeieškojo jo, tikėdamosi užverbuoti savo kampanijai, nukreiptai prieš kibernetinius nusikaltimus.

Cyrikas buvo kvintesencinė kibernetinio pogrindžio figūra – jis atsirado tarsi nežinia iš kur; jis demonstravo neribotą, netgi galima sakyti – nemalonią arogranciją; tačiau jo motyvacija leisti valandų valandas rašant pranešimus, dalyvaujant dažnai bergždžiose diskusijose ir agituojant savo bendraminčius vis tiek buvo sunkiai suvokiama.

Iki tol, kol Mertas Ortaças neatskleidė, kad du aktyviausi Turkijos naujai užgimusios internetinių skelbimų paslaugos naudotojai turi slapyvardžius Cha0 ir Lordas Cyrikas, niekas net nebuvo bandęs sujungti šių dviejų gijų.

Naudodamasis savo išskirtinio žavesio ir dviveidiškumo deriniu, vėlyvą 2007 m. pavasarį, pasiskelbęs internete slapyvardžiu PilotM, Mertas prisistatė Lordui Cyrikui kaip jo ir Cha0 bendras pažįstamas. „Ei, seni! – rašė jis jam, – ką veiki šitame forume?“ Vyrukui, apsimetusiam jo senu draugu, Cyrikas labai troško užduoti tokį pat klausimą! Taigi greitai jie patenkinti plepėjo, ypač šifravimo tema. Mertas pastebėjo, kad Lordas Cyrikas yra nepaprastai talentingas kompiuterių inžinierius, o tai patvirtino jo nuojautas apie tikrąją veikėjo asmenybę. Kelias dienas ar savaites keitęsis idėjomis ir informacija, Cyrikas sutiko padėti surengti virtualų Cha0 susitikimą su Mertu (kuris vis dar apsimetinėjo kai kuo kitu). Naudodamasis užkoduotomis keitimosi informacija programos „Icq“ žinutėmis, Mertas pradėjo kalbėtis su Cha0 (be abejo, turkiškai).

„Paklausyk, – pasakė Cha0 Mertui, – aš neleidžiu daug laiko Turkijoje. Man geriau patinka užsienis, – dėstė jis ir prisipažino nelabai mėgstantis savo tėvynainių ir kiek įmanoma vengiantis turėti su jais reikalų. – Mano vardas Şahinas ir aš kalbu turkiškai tik tada, kai tai būtina. – Jis buvo pasiruošęs kalbėtis su Mertu turkiškai tik todėl, kad juos vieną kitam pristatė Lordas Cyrikas. – Mes su juo esam labai seni draugai“, – pasakė Cha0.

2007-ųjų balandį Cha0 iš Tamsiosios rinkos išmetė Droną su visais jo sugebėjimais į nelegalius Cha0 skaitytuvus įmontuoti

mikroprocesorius. Tada paklausė Merto, ar šis negalėtų to daryti, ir Mertas sutiko. Dabar jis jau rimtai įsitraukė į Cha0 kriminalinį verslą, o tai reiškė, jog pradėjo kaupti pačią vertingiausią prekę – pasitikėjimą.

Tik Mertas galėjo tvirtinti turįs artimų ryšių su Cha0 ir Cyriku. Šiuodu, be abejo, negalėjo tvirtai teigti, jog susirašinėja su Mertu, nes jis apsimetinėjo kai kuo kitu. Cha0 atvirai neigė kada nors pažinojęs Mertą ar su juo bendravęs – iki tos lemtingos dienos, kai prievarta jį pagrobė ir per „Haber 7" įkėlė jo nuotrauką į internetą.

Dar svarbiau buvo tai, kad niekas Turkijoje ar kur nors kitur niekada nepatvirtino paslaptingojo Şahino egzistavimo. Už Merto pasaulio ribų nėra jokių įrodymų, kad Şahinas egzistavo ar egzistuoja ir kad juodu galiausiai susitiko. Bet Mertas pasirodė esąs teisus dėl vieno svarbaus fakto: Lordo Cyriko ir Cha0 draugystė buvo nuėjusi ilgą kelią.

Mertas, be abejo, tebedirbo Turkijos žvalgybos agentūrai. Taigi, didelę dienos dalį vaidinęs, jog dirba Turkijos „Fox" televizijai, ir užsiiminėjęs Tamsiosios rinkos reikalais arba modeliavęs mikroprocesorius Cha0 nelegaliai kortelių duomenų nuskaitymo industrijai, Mertas vakarais dažniausiai pateikdavo savo vadovams ataskaitas apie tos dienos radinius. Jis pasakodavo jiems apie lenką elektroninio brukalo siuntinėtoją, pasivadinusį Meistru Splyntru, apie apsaugos sistemų genijų Grendelį, apie Lordą Cyriką ir Cha0, apie atsarginius serverius, kuriais Tamsiosios rinkos administratoriai naudojasi įvairiose Europos šalyse, ir apie DHKP-C veiklą.

Kuo dar jis užsiėmė? Jo viršininko iš Turkijos „Fox" televizijos įtarumas vis augo. Jis pastebėjo, kad dabar Mertas beveik niekada neatlieka jam skirtų užduočių, bet amžinai pateikia litanijas pasiaiškinimų, kodėl nebuvo darbo vietoje. Jis tvirtindavo turėjęs rimtų sveikatos problemų ir nuolat mėgindavo skolintis pinigų iš kolegų. Jei jam taip sekasi, stebėjosi viršininkas, kodėl jis amžinai neturi pinigų?

Vieną dieną viršininkas išsiaiškino, kad Mertas prašė visų bendradarbių slaptažodžių. Esą jie buvo jam reikalingi, kad galėtų įvykdyti svarbius sistemos patobulinimus. Viršininkas pačiu laiku sustabdė šį planą, įtaręs, kad slaptažodžiai Mertui reikalingi ne tokiems garbingiems tikslams.

Kitą dieną, tyliai stebėdamas Mertą, ant jo stalo viršininkas pamatė šūsnį kreditinių kortelių. Vėliau užtiko dvi Merto asmens tapatybės korteles, iš kurių nė vienoje nebuvo įrašytas tikrasis jo vardas ir pavardė, gimimo data ir vieta. Galiausiai jis pastebėjo, kaip Mertas naršo po interneto svetainę su smulkiomis instrukcijomis, kaip įsilaužti į bankomatą. Kuo ilgiau Mertas užsibūdavo, tuo labiau jam reikėjo pinigų – ir dargi didelių sumų.

Mertas susipažino su Sanem – svajonių moterimi, dėl kurios pametė galvą. Sanem – vienintelis žmogus pasaulyje, galintis patvirtinti, ar išskirtinė Merto istorija yra tiesa, ar ne. Bet Sanem tyli.

32
Turkiški malonumai

„Sükrü Saracoğlu“ stadionas triukšmingame Azijos pusėje esančiame Stambulo Kedikejaus rajone buvo pilnas žmonių, skubančių į finalines „Fenerbahçe“ futbolo klubo sezono rungtynes namuose. „Fenerbahçe“ jau buvo laimėjęs aukščiausioje lygoje, taigi šios rungtynės, vykstančios puikų gegužės pabaigos sekmadienį, buvo tiesiog triukšminga šventė patiems fanatiškiausiems futbolo sirgaliams pasaulyje.

Į šią šventę atžygiavo ir Mertas Ortaças. Gal iš tiesų, o gal tik savo vaizduotėje.

Aukštai išdėstytose prabangiose ložėse vyravo šventiška laukimo nuotaika. Şahinas ir jo patikimas padėjėjas Çağatay'us Evyapanas laukė pirmojo žaidimo smūgio iš aikštės vidurio; žaidimas turėjo prasidėti penktą valandą po pietų. Stambulo futbolo sirgaliai buvo laikomi vienais iš fanatiškiausių visoje Europoje. Jie buvo susiskirstę į tris stovyklas. Dvi stovyklos buvo europinėje miesto dalyje – tai „Galatasary“ ir „Beşiktaş“ klubų sirgaliai, o geltonos ir tamsiai mėlynos spalvų marškinėlius vilkintys „Fenerbahçe“ žaidėjai buvo garbinami sąsiaurio Azijos pusėje. Şahinas ir Çağatay'us buvo atsidavę „Fenerbahçe“ komandos sirgaliai, o pastarojo apsilankymai savo gimtajame mieste paprastai sutapdavo su rungtynėmis – ir, be abejonės, stadione jis turėjo savo ložę.

Tarp kitų draugų, pakviestų į šias rungtynes, buvo ir Mertas, kuris, kaip Şahinas pasakė Çağatay'ui, buvo vienas iš naujų vaikinų, dirbančių jo nelegalių skaitytuvų versle. Mertas pristatė jiems savo

naująją draugę Sanem. Ji buvo susukusi galvą Mertui, o ją svaigino demonstratyvus jo kompanionų turtingumas.

Sanem jau žinojo pagrindinius faktus apie kai kuriuos ložėje sėdinčius žmones. Meilikavimu išgauti paslaptis iš Merto jai nebuvo sunku. Jis ne tik iš prigimties buvo šnekutis, bet ir nepaprastai troško padaryti įspūdį savo jaunajai meilužei, kurią laikė daug pranašesne už save. Tokių galingų vyrų kaip Şahino ir jo tvirtai sudėto bendro Çağatay'aus išdidus vaikščiojimas po prabangią ložę turėjo patvirtinti Sanem, kad mažasis Mertas iš tiesų turi įspūdingų bičiulių. Tad gal „Fenerbahçe" rungtynės vis dėlto nebuvo Merto vaizduotės vaisius.

Gyvenimas Mertui buvo dosnus. Jie su Sadunu apgaudinėdami „Akbank" banką pradėjo uždirbti rimtus pinigus. Būdamas aktyvus Nacionalinės žvalgybos informatorius, jis turėjo visapusišką apsaugą, be to, jį labai vertino pagrindinis Tamsiosios rinkos veikėjas Cha0. Ir, be viso kito, jis visas dienas ir naktis leido su pasakiškai gražia jauna mergina, kuri, atrodo, buvo įsimylėjusi jį taip pat, kaip ir jis ją.

Atėjus vasarai, Mertas nusprendė pasinaudoti palankia lemtimi ir užsisakyti atostogas Antalijoje savo taip trokštamame „Adam & Eve" viešbutyje, kur projektuotojai buvo „sėkmingai suderinę" didelį biudžetą su itin prastu skoniu. Daugybė baseinų tyvuliavo vestibiulyje su visą laiką besikeičiančiais šviesos efektais, o kambariai garsėjo nesuskaičiuojama daugybe veidrodžių, skatinančių daug energijos reikalaujantį seksą. Visa tai kainavo nepigiai. Kambarių kainos prasidėjo nuo 400 dolerių už naktį, o lankytojai buvo pastebėję, jog labai greitai jų sąskaitos smarkiai išauga dėl papildomų paslaugų. Bet jauniems, gražiems ir turtingiems Turkijos piliečiams tai buvo vasaros sezono atostogų tikslas.

Vos tik Mertas su Sanem įsiregistravo, jie susidūrė su Çağatay'umi, kuris taip pat buvo atlėkęs į pietus vasaroti. Mažam

akiniuotam storuliui, lydėjusiam jį, Çağatay'us paaiškino, kad Mertas padeda Cha0 komandai tvarkyti „administracinius reikalus". Storas kaip kubilas džentelmenas pažvairavo į Mertą ir sušuko: „Lukterk minutėlę. Aš pažįstu šitą vyruką nuo tada, kai jis bėgiojo su trumpikėmis! Ką, po velnių, tu veiki šiame versle?" Mertas, kaip visada, atsakė kikenimu ir pašaipia šypsenėle.

Įėjęs su Sanem į miegamąjį, Mertas palinko virš jos ir pasakė: „Kas tas antras vyrukas? Tai Lordas Cyrikas." Sanem norėjo sužinoti, ar Cyrikas galingesnis už Cha0. Mertas patikino ją, kad ne; jis prisiminė, kad ją pirmiausia domina galia, o tik paskui pinigai.

Mertas buvo iki ausų įsimylėjęs ir jautėsi esąs devintame danguje. Jis buvo pinigingas, vienodai gerbiamas tiek nusikaltėlių, tiek žvalgybos tarnybos, o viešajame pasaulyje turėjo įspūdingą darbą – vadovavo Turkijos „Fox" televizijos Informacinių technologijų skyriui. Dar daugiau, vasarą jis dykinėdamas leido „Adam & Eve" viešbutyje su savo naująja karšta panele. Nieko geriau nė negalėjo būti. Ir nebebuvo – žvelgiant į praeitį, 2007 m. rugpjūtis buvo Merto Ortaço fantazijų pasaulio aukso amžius, kai jo svajonių planai bent sykį sutapo su tikrove. Beveik tuoj pat, kai grįžo į Stambulą, reikalai pradėjo slysti jam iš rankų, ir, rudeniui pakeitus vasarą, aplink jį ėmė kauptis tamsūs debesys. Norėdami apsipirkti, Sanem ir Mertas buvo pratę leistis į brangias keliones, tokias vietas kaip Mikono sala kaimyninėje Graikijoje. Pora per dieną iššvaistydavo tūkstančius eurų, o tai patuštindavo net ir Merto gerai prikimštą lobių skrynelę. Jį pradėjo piktinti, jo manymu, per didelis jos išlaidumas, o ji vis labiau irzo dėl jo paslapčių ir melagysčių.

Per vieną painų epizodą Mertas buvo sulaikytas, įtarus, jog iš Sanem brolio draugo pavogė 5 000 eurų. Jo sulaikymas buvo paskutinis lašas, perpildęs „Fox" kompanijos kantrybės taurę, ir jis buvo atleistas iš darbo. Dar blogiau, Nacionalinė žvalgyba galiausiai nusprendė, kad jis tapo našta ir jo nebeverta saugoti. Kaip perkūnas

iš giedro dangaus jį užgriuvo suvokimas, kad, netekęs dviejų svarbių pajamų šaltinių, jis tapo labai nesaugus.

Paleistas už užstatą, jis paspartino kardingo veiklą su Sadunu, pasinaudodamas tuo, kad „Akbank" sistema vis dar pažeidžiama. Neviltis erzino, o ją dar sustiprino nemaloni žinia, kad Sanem turi romaną. Paskesnį santykių nutrūkimą lydėjo audringi abipusiai priekaištai ir kartūs kaltinimai. Mertas buvo įsitikinęs, kad ji pavogė iš jo didžiules pinigų sumas. O ji greičiausiai manė, kad jis paprasčiausiai pamišęs.

Merto pasauliui staiga pradėjus byrėti, prieš pat Naujuosius metus jis iškeliavo į pietus, norėdamas apsvarstyti savo tolesnius žingsnius. Kelyje jis vėl sužinojo blogų naujienų – Sadunas suimtas, o policija, mojuodama sulaikymo orderiu, jau atliko kratą jo bute. Jei būtų likęs Stambule, jis jau sėdėtų už grotų. Kaip dažniausiai būna atsidūrus sunkioje situacijoje, Mertas nusprendė įsikasti dar giliau, kol iš tikrųjų patikimai pasislėps pogrindyje.

Grįžęs į Stambulą jau su kita, fiktyvia, pavarde, jis pradėjo kurti pabėgimo strategiją. Pasinaudojęs viena iš daugelio savo padirbtų asmens tapatybės kortelių, jis kreipėsi dėl naujo paso ir gavo jį, o tada papirko Prancūzijos ambasados konsulato pareigūną, kad gautų vizą. Paskui leidosi į vingiuotą kelionę: per Prancūzijai priklausančią Karibų jūroje esančią Martiniką, tada per Paryžių į Alesą – snaudžiantį miestelį, esantį už penkiasdešimties mylių į šiaurę nuo Prancūzijos Viduržemio jūros pakrantės.

Mertas buvo izoliuotas. Turėjo nedaug pinigų, vargiai išlemeno kokį žodį prancūziškai ir, dar blogiau, neturėjo prieigos prie interneto. Bet jis bent jau galėjo pasiguosti, kad yra saugus. Taigi, neturėdamas ką daugiau veikti, Mertas nusprendė gerai pailsėti ir atsipalaiduoti.

Po beatodairiško bėgimo nuo Turkijos teisėsaugos ir kivirčų su buvusia mylimąja Aleso miestelis jam greitai ėmė atrodyti malonus

prieglobstis. Pirmą sykį po daugelio mėnesių, o gal ir metų, jis galėjo apsieiti be pusiau tiesos sakymo, apgavysčių, vagysčių ir išsisukinėjimų. Jam nebereikėjo būti padalytam į visiškai skirtingas asmenybes, kaip reikalavo šitas daugialypis internetinis ir realusis pasaulis, ir ieškoti savo tikrosios esmės – žinoma, jei jos dar nebuvo praradęs ir ją dar buvo galima atpažinti. Galbūt atėjo laikas atsikvėpti nuo beprotybės: laikas nustoti elgtis nedorai, laikas rasti tinkamą darbą ir įsikurti su padoria moterimi. Jei būtų išmintingai viską susidėliojęs, visa tai būtų buvę pasiekiama.

O tada vieną rytą, apie aštuntą valandą, pasigirdo beldimas į duris.

Mertas gulėjo lovoje ir siurbčiojo kavą. Čia, Alese, jis dar niekada nebuvo sulaukęs svečių ir nesitikėjo jų sulaukti. Užsimetęs chalatą, jis nušlepsėjo prie durų, o atidaręs jas pamatė du vyriškius su kuprinėmis. „Sveikas, Mertai! Kaip laikaisi?“ – pasakė pirmasis turkiškai. Atsakydamas Mertas nedrąsiai sumurmėjo: „*Je ne comprends pas...*“* „Baik, Mertai, – pratarė antrasis vyrukas angliškai, – mes žinom, kas tu toks. Turėtum pasikviesti mus į vidų.“

Jiems besėdint virtuvėje su puodeliais kavos, vienas vyriškis išsitraukė aplanką ir padėjo jį ant stalo. Mertas nusprendė, kad pirmasis vyriškis yra antros kartos imigrantas, atvykęs į Ameriką iš Turkijos, nes kalbėjo šnekamąja turkų kalba, bet su akcentu, ir retsykiais padarydavo gramatinių klaidų. Antrasis vyriškis, kuris kalbėjo daugiausia, buvo amerikietis.

Mertui buvo pateiktos dvi alternatyvos: „Arba tu besąlygiškai padėsi mums, arba mes perduosime šį aplanką saugumui.“ Mertas akimis permetė puslapius su prancūziškų kreditinių kortelių duomenimis, kuriuos juodu su Sadunu buvo nuskaitę, įsiskverbę į banko „Akbank“ kompiuterinę sistemą. Svečiai jam priminė, jog Pran-

* Aš nesuprantu. (Pranc.)

cūzijoje už apgavystę tik su viena kreditine kortele jis gali gauti iki aštuonerių metų.

Mertas neturėjo iš ko rinktis, bet prieš sutikdamas pareikalavo, kad vyrai pasisakytų, kam jie atstovauja.

– Amerikos teisėsaugai, – pasigirdo atsakymas.

– O ko, – klausinėjo Mertas, – jūs norit iš manęs?

– Nagi, Mertai, spėk drąsiai!

Susierzinęs ir išsigandęs Mertas papurtė galvą.

– Mes norim, kad tu mums išduotum Cha0.

33
Sugrįžimas į pragarą

Kol trys vyrai kalbėjosi apie Cha0 ir galimą jo buvimo vietą, iš klausimų ir komentarų Mertas suprato, kad jie nepažįsta nei Cha0, nei Lordo Cyriko. Du agentai pasakė Mertui, kad jam teks sugrįžti į Turkiją, atkurti narystę Tamsiojoje rinkoje ir išstumti iš jos Cha0 ir jo bendrus. Jie dar labiau jį nustebino pareiškę, kad vienas iš jų žmonių kontroliuoja Tamsiosios rinkos serverį. Taigi jie lengvai gali padėti jam sugrįžti į forumus.

Kiek Mertas sugebėjo išsiaiškinti, FTB dabar norėjo prasibrauti prie likusių pagrindinių Tamsiosios rinkos veikėjų: Cha0, Lordo Cyriko, Meistro Splyntro, Štirlico ir Grendelio. Jie dar nepasakė, kaip konkrečiai tai bus padaryta, bet akivaizdu, jog tvarkydami visą šitą reikalą tikėjosi pasinaudoti juo kaip pagrindiniu įrankiu. Tokia perspektyva jo nė kiek netraukė, kaip ir perspektyva kažkiek laiko praleisti kokiame nors Prancūzijos kalėjime, apie kuriuos kalbama, kad jie vieni iš griežčiausių Vakarų Europoje.

Amerikiečiai agentai davė Mertui keletą miglotų pažadų ir įteikė jam Lucy Hoover, atašė padėjėjos teisės klausimais prie JAV ambasados Stambule, telefono numerį ir elektroninio pašto adresą. Jie taip pat paskyrė jam elektroninio pašto adresą sadinsider@gmail.com (vardą Mertas pasirinko pats), iš kurio jis galėjo rašyti jai žinutes.

Merto laikinas apsigyvenimas Langedoke yra antras jo fantazijų pasaulio epizodas, kurio neįmanoma patikrinti. Tačiau jis iš tiesų susisiekė su Lucy Hoover iš FTB, kuri tuo metu buvo Turkijoje.

Į Turkiją Mertas grįžo 2008 m. kovo 2 d., po dviejų mėnesių nuo savo išvykimo. Pirmiausia jis turėjo sudaryti veiksmų planą. Jis nusprendė kreiptis į naujienų agentūrą ir televizijos stotį „Haber 7" ir pasiūlyti jiems duoti interviu, kuriame pažadėjo atskleisti kardingo pasaulio ir Tamsiosios rinkos paslaptis. Jo tikslas, nors gal ir neišmintingas, buvo įbauginti Cha0, kad šis žinotų, jog informacija apie jo operaciją nuteka ir, galimas dalykas, juo domisi policija.

Būdamas naivus – o tai vis dėlto buvo svarbi jo charakterio savybė – Mertas įsivaizdavo, kad Cha0 nesugebės nustatyti, kas iš tiesų yra tas programišius, pasisiūlęs duoti interviu žiniasklaidai. Bet Mertas nesitikėjo, kad žmogus iš „Haber 7" paslapčia nufotografuos jį Kedikejaus rajono „McDonald's" restorane, kur jis susitiko su jų žurnalistu. Kai tik nuotrauka buvo išspausdinta, Cha0 suprato, kas prasitarė. Mertas rimtai pakliuvo į didžiojo vyro akiratį.

Kadangi jau buvo išduotas orderis Mertui suimti, o Sadunas sėdėjo už grotų, Cha0, Lordas Cyrikas ir kiti greičiausiai žinojo, kad Mertas bijo teisėsaugos spaudimo. Interviu tik sustiprino šiuos įtarimus. Taigi užuot sugrįžęs tiesiai į Tamsiosios rinkos forumą, Mertas susisiekė su savo jaunu bičiuliu programišiumi vardu Mustafa, kurį Cha0 taip pat pažinojo. Apie Mustafą buvo kalbama, kad jis trokšta ištobulinti savo įgūdžius lengvai užsidirbti pinigų iš kardingo ir kibernetinių nusikaltimų.

Mustafos šeima buvo kilusi iš Antalijos, o tai Mertui suteikė progą išvykti iš Stambulo, kur jautėsi nesaugus. Sugrįžęs į savo mėgstamą šalies pietinę dalį, jis ten praleido daugiau nei mėnesį.

Mustafa dirbo Tamsiojoje rinkoje, prisidengęs slapyvardžiu MYD. Jo darbiniai santykiai su Cha0 buvo geri. Tačiau Mertas nežinojo, kad Mustafa buvo perspėjęs Cha0, jog Mertas pasirodė ir jį persekioja.

Mustafa suorganizavo susitikimą su Cha0 Stambule, taigi juodu su Mertu vėl grįžo į šiaurę. Mertas tolydžio informuodavo

Lucy Hoover apie savo judėjimą ir perspėjo ją, jog ruošiasi susitikti su Cha0. Amerikiečiai norėjo stebėti Cha0 ir nustatyti jo buvimo koordinates ir ryšių infrastruktūrą. Mertas šį sykį laikėsi pažado atvesti amerikiečius pas jų persekiojamąjį. Cha0 davė nurodymus Mustafai susitikti su jo žmonėmis prie mėsainių restorano „Burger King" netoli Stambulo *Göztepe* priemiestinių traukinių stoties, kuri yra Azijos pusėje, už poros mylių nuo „Fenerbahçe" stadiono.

Pasiekę *Göztepe*, jie pamatė Haktaną Öztaną, didelį kaip bulius vyrą, kuris buvo Çağatay'aus asmens sargybiniu, kai jie kartu sėdėjo kalėjime, o dabar pasiūlė tokias pat paslaugas ir Şahinui. Asmens sargybinis nuvežė juos abu į daugiabutį pavadinimu „Sözdener Apartments", esantį maždaug už dviejų mylių, turtingame vidurinės klasės rajone Suadijėje. Kambariai buvo gana menkai apstatyti ir ne itin patrauklūs. Haktanas dviem vyriškiams liepė likti vietoje ir pasakė, jog kai kas užmegs su jais ryšį.

Nesaugomas atvirų erdvių ir nebeglobojamas Nacionalinės žvalgybos, dabar Mertas išsigando, kad Çağatay'us ruošiasi su juo susidoroti. Mertui nežinant, pagal Cha0 nurodymus Mustafa buvo paleidęs trojaną į jo nešiojamąjį kompiuterį, taigi dabar Cha0 iš užkrėsto kompiuterio galėjo sužinoti visas tankių Merto dviveidiškumo džiunglių paslaptis. Cha0 buvo ne tik kriminalinio pasaulio meistras, jis taip pat nieko nedovanodavo. Dabar jis turėjo svarių įrodymų, kad Mertas dirba policijai. Mertas manė (ir, be abejo, tikėjosi), kad Lucy Hoover bus ką nors suorganizavusi, kad butas būtų sekamas, bet nepastebėjo jokių tai patvirtinančių ženklų. Taigi, jei staiga pasirodytų Çağatay'us, Şahinas ir Haktanas, po vieną ar keliese, jis atsidurtų rimtame pavojuje.

2008 m. gegužės 18 d., sekmadienį, dešimtą valandą ryto, kai Mertas buvo vienas „Sözdener Apartments" daugiabutyje, sučiršKė durų skambutis. Jis atidarė ir pamatė priešais stovintį Haktaną. Lankytojas be žodžių smarkiai pražingsniavo pro jį, užtrenkęs

paskui save duris. Mertas džiugiai pareiškė, jog tikėjosi jį pamatyti. Haktanas rūsčiai pažvelgė į jį. „Minutėlę“, – tarė jis. Tada atidarė duris ir įleido Çağatay'ų. Merto veidas iš raudono tapo violetinis, paskui – baltas.

Çağatay'us pastūmė Mertą į kėdę ir pradėjo lėtai vaikščioti pirmyn ir atgal priešais jį, monotoniškai tarsi ritualą kartodamas: „*Mert... Namert... Mert... Namert*“, – tai turkiškų žodžių žaismas, kur antonimas žodžiui *mert* (drąsus) yra *namert* (bailus).

Paskui Mertas atsidūrė ant grindų ir buvo spardomas į pilvą, krūtinę ir kojas. Įėjo dar du stambūs vyrai, užmetė jam ant galvos antklodę, kad jis negalėtų jų atpažinti, ir taip pat ėmė jį mušti. Retkarčiais Mertas žvilgsniu pagaudavo į galvą nukreiptą ginklą.

Mertas nualpo. Atsigavęs suprato tebegulįs ant grindų, bet pastebėjo, jog kažkas su vaizdo kamera filmuoja viską, kas vyksta. Užkrėtęs Merto nešiojamąjį kompiuterį trojanu, Cha0 ne tik sugebėjo išgauti informaciją apie jo santykius su Lucy Hoover, bet ir galėjo išsiaiškinti, kad Merto paslaugomis naudojosi Nacionalinė žvalgyba (nors tik iš dalies sėkmingai).

„Gerai, – tarė Çağatay'us, tarsi koks ceremonimeistras paspausdamas įrašymo mygtuką. – Dabar tu papasakosi mums visą istoriją nuo pradžios iki galo.“ Ir taip Mertas papasakojo savąją pasakos „Veidrodėlis“ versiją, o baigė apie trečią valandą ryto. Jie norėjo žinoti viską – apie šnipus, apie kardingą su Sadunu, apie Tamsiosios rinkos tyrinėjimus, apie jo merginą – nė viena smulkmena nebuvo pamiršta.

Galiausiai banditai sumigo, bet vienas iš jų visą laiką budėjo, kad užtikrintų, jog jei tik Mertas užsnūs, spyrių ir smūgių kruša galės jį pakelti.

Pirmadienį apie pietus paskambino Şahinas. Çağatay'us padavė jam telefoną su įjungtu garsiakalbiu. Iki to laiko Merto valia jau buvo palaužta. Jis manė, jog bus nužudytas. Mertas nenustebo, kai

Şahinas liepė jam pakartoti viską, ką jau buvo pasakęs. Viskas buvo nufilmuota. Galiausiai Şahinas prakalbo. „Gerai, o dabar atėjo laikas bausmei, – pasakė jis be jokios ironijos. – Aš noriu, kad darytum viską, ką tau lieps Çağatay'us, o aš įvertinsiu rezultatą."

Çağatay'us liepė Mertui atsistoti ir nusirengti. Išsigandęs, kad jį grupiniu būdu žagins, Mertas galiausiai pratrūko. „O, dėl Dievo meilės, geriau tiesiog paleiskit kulką man į kaktą, – maldavo jis. – Ką, po velnių, manot su manim daryt?"

„Užsičiaupk, – atkirto Çağatay'us. – Tau nėra ko nerimauti. Mes ne kokia gėjų šutvė. Lik su trumpikėmis ir priimk bausmę!" Tebekalbėdamas telefonu su Şahinu, Çağatay'us keverzojo liūdnai pagarsėjusiame popieriuje, kuriame Kieras, arba Mertas Ortaças, buvo išvadintas išdaviku ir skundiku. Taip buvo sukurtas mitas apie Kierą. Žurnalistas iš „Haber 7" buvo radęs Merto vardą interneto svetainėje kartu su slapyvardžiu „Kieras". Iš tiesų Mertas niekada nesinaudojo šiuo vardu ir neketino to daryti – jo tikrasis slapyvardis buvo SLayraCkEr. Bet kai Çağatay'us jį nufotografavo, žurnalistai, policija ir karderiai visame pasaulyje pradėjo Mertą Ortaçą vadinti Kieru, nors gyvenime jis niekada nebuvo taip vadinamas.

Po fotosesijos Mertas vėl buvo partrenktas ant grindų ir ant jo buvo užmesta antklodė. „Pabūk čia pusvalandį, o tada galėsi išeit, – pasakė Çağatay'us. – Mes tau paliekam drabužius ir neliesim tavo pinigų. Gali pasiimt ir vieną asmens tapatybės kortelę. Nuo dabar – visą likusį gyvenimą – nė nemanyk ištarti Cha0 vardo, nes jei taip padarysi, aš pasmaugsiu tave plikom rankom, tau nė nespėjus įkvėpti." Galiausiai Çağatay'us neatsispyrė nepridėjęs pastabos: „Jei tai priklausytų nuo manęs, nudėčiau tave čia ir dabar. Bet vyrukui tu patinki. Būk jam dėkingas ir neprasižiok." (Iš tiesų pačiam Çağatay'ui net mintis apie tai, kad jis galėtų nužudyti tokį kaip Mertas – jo akimis, smulkų niekšelį – atrodė juokinga.)

Po pusės valandos sudaužytas Mertas Ortaças tik su penkiasdešimčia dolerių kišenėje klupinėdamas išėjo iš buto ir pasuko link autobusų stoties, iš kur nuvažiavo į Izmiro miestą. Čia jis laižėsi savo žaizdas ir galvojo, ką, po galais, jam daryti toliau. Buvo akivaizdu, kad teks pasislėpti pogrindyje. Taigi Mertas išnyko paskutinį kartą – iki tol, kol po daugelio mėnesių, 2008-ųjų lapkritį, buvo suimtas kreipdamasis dėl paso, kurį norėjo gauti kitu vardu ir pavarde.

Yra išlikę ir daugiau keistų pasakojimų iš Merto vizijų pasaulio – nesuprasi, ar tai tiesa, ar fantazijos, – bet turėdami savų tikslų juos čia ir baigsime.

34
Turko medžioklė

Iki tol, kol Mertas galiausiai buvo suimtas, inspektorius Bilalas Şenas neturėjo jokio supratimo, ar programišius pabėgęs, ar vis dar įkalintas, ar paprasčiausiai numirė. Tačiau jis žinojo, kad laikas eina jo nenaudai. Pareigūnui nebuvo iš ko rinktis – reikėjo ir toliau kuo veiksmingiau ir kantriau tęsti Cha0 paieškas. Dabar jis bent jau turėjo žmogaus, siuntusio nelegalų skaitytuvą, nuotrauką ir telefono numerį ir buvo tikras, kad tai galiausiai atves jį pas Cha0. Kadangi pasiuntinys, įteikęs skaitytuvą, naudojosi vienu iš telefono numerių, kuris priklausė vežėjų kompanijai, policija galėjo užspeisti įtariamąjį – kitaip tariant, jie galėjo atpažinti, kokias mobiliųjų telefonų antenas prietaisas pasiekia. Netrukus jie tiksliai žinojo, kur jis yra ir kaip juda.

Veikiai jie pastebėjo jį antrą kartą ir galėjo pasekti. Kaip ir reikėjo tikėtis, per keletą dienų žmogus juos atvedė į tolimą Stambulo priemiestį Tuzlą, esantį maždaug už penkiolikos mylių nuo Stambulo, azijinės dalies pakrantėje. Ši vietovė, kurioje išsidėsčiusios didžiausios Turkijos jūrų laivyno bazės ir kuri kadaise garsėjo žvejyba, buvo viena iš nedaugelio miesto sričių, kur dar nevyravo nauji pastatai. Tai buvo labai populiarus gyvenamasis rajonas su spalvingais namais, kuriuose daugiausia įsikūrusios turtingos šeimos.

Įtariamasis atvedė juos prie prabangios vilos su lauke įrengtu baseinu. Keletą dienų stebėjusi, sekimo komanda įsitikino, kad viloje gyvena keli vyriškiai. Tačiau Bilalas netruko nustatyti, kas jiems duo-

da nurodymus. Peržiūrėjęs nusikaltėlių įrašus, jis greitai išsiaiškino, jog tai kažkoks Çağatay'us Evyapanas. Talentingas koledžo elektros inžinerijos studentas Çağatay'us dabar savo įgūdžius taikė realiame gyvenime. Pirmą sykį jis buvo suimtas už sukčiavimą 1998 metais. Po dvejų metų jis labiausiai prašovė, kai su savo bendrininkais buvo pagautas nusikaltimo vietoje su klonuotomis plastikinėmis kreditinėmis kortelėmis imantis pinigus iš Izmiro uosto bankomatų. Atsėdėjusiam penkerius metus iš paskirtos dvidešimt septynerių metų bausmės, tolesnio įkalinimo perspektyva jam atrodė nepakeliama. Taigi vieną 2005 m. gegužės dieną Çağatay'us perlipo per kalėjimo sieną, išvengęs radaro. Jis labiau panėšėjo į vėlę nei į pabėgėlį.

Dėl savo 2000 m. arešto jis kaltino vyriškį, su kuriuo kartu dirbo, taigi ryžtingai apsisprendė niekada nebeleisti, kad taip dar kartą įvyktų. Jei nori ką nors padaryti deramai, vadovaukis Çağatay'aus filosofija ir daryk tai pats.

Jis, be abejo, suprato, kad per tuos penkerius metus, kol sėdėjo kalėjime, kibernetinis pasaulis labai pasikeitė. Jis žinojo Moore'o dėsnį, numatantį, kad tranzistorių skaičius, kuris gali būti nebrangiai sutalpintas mikroschemoje, maždaug iki 2015-ųjų dvigubės kas dvejus metus. Realiame gyvenime šis dėsnis reiškia, kad kasmet elektroniniai prietaisai taps modernesni, kompiuteriai ir jų programos – sudėtingesnės, įsilaužimo priemonės – įmantresnės, o ir atlygis atitinkamai didesnis. Taigi jis nusprendė prisitaikyti prie naujų aplinkybių.

Pirmiausia jam reikėjo naujos tapatybės kibernetinėje erdvėje. Çağatay'us išnyko beveik ketveriems metams, jo vardas ir pavardė pase buvo pakeisti vieno iš jo pavaldinių, asmens sargybinio Hakano Öztano, vardu ir pavarde, o internetinėje erdvėje jis pasivadino Cha0 slapyvardžiu (tariamu kaip itališkas pasisveikinimas). Jis naudojo pirmą žodžio skiemenį ir skaičių nulis nuo tada, kai praeito amžiaus paskutiniame dešimtmetyje pirmą kartą savo apsilankymu pagerbė

internetinių skelbimų lentos paslaugų svetaines. Tuo metu išskirtinė Cha0 saugumo sistema leido užtikrinti, kad niekas negalės nustatyti jo tapatybės. Tokiuose viešuose forumuose kaip „CrimeEnforcers" ir „DarkMarket" Cha0 pardavinėjo nelegalius skaitytuvus. Privačiai jis pardavinėjo neįveikiamas saugumo sistemas tiems kompiuterių vartotojams, kurie iš tiesų nenorėjo, kad jų asmenybė būtų atskleista.

Bet dabar Bilalas jį netikėtai aptiko. Tačiau viena buvo nustatyti Cha0 buvimo vietą. Visai kas kita – surinkti būtinus įrodymus, kurie leistų iškelti jam bylą. Turkijos teisėjai ir prokurorai yra dar mažiau susipažinę su internetu nei jų kolegos Vakarų Europoje ar Amerikoje, tačiau mieste jau buvo keletas žymių ir brangių advokatų, kurie greitai mokėsi panaudoti šitą neišprusimą savo klientų naudai, o kartu padidinti savo pačių banko sąskaitų likučius.

Çağatay'us džiaugėsi vasara – jis buvo kompanijas mėgstantis vyrukas, kuriam patiko linksmai leisti laiką su draugais. Jį dažnai buvo galima pamatyti lydintį gražias moteris, tarp jų, sklido gandai, vieną drąsią Saudo Arabijos karališkosios šeimos narę. Jis mėgo brangius gėrimus, gerus valgius, mėgo dalyvauti jachtose rengiamuose vakarėliuose ir, metams bėgant, buvo priaugęs šiek tiek svorio. Atrodė, jog jam nestinga pinigų, kad galėtų gyventi prabangiai.

Bilalas ėmė sekti įvairius Çağatay'aus bendrininkus – jam kilo įtarimų, kad po Cha0 slapyvardžiu slepiasi ne tik pats Çağatay'us Evyapanas, bet ir visas gerai veikiantis nusikaltėlių sindikatas. Tai buvo organizuoti nusikaltimai, o ne kokių nors paauglių programišių pirmieji įsilaužimai į serverius. Jie taip pat liudijo augančią pasaulinę tendenciją. Ilgą laiką tradiciniai organizuotų nusikaltėlių sindikatai sukčiavimą internete laikė menku nusikaltimu, nelabai vertu dėmesio. Dabar viskas pradėjo keistis. Persikėlę iš savo originalaus inkubatoriaus, kur kikena ir žaidžia išdykę kompiuterių fanatikai, į brandesnį pasaulį su realiomis mafijos struktūromis, kibernetiniai nusikaltimai darėsi sistemingesni, efektyvesni ir buvo

vykdomi su didesne apsauga. O tai reiškė, kad Bilalo grobis atitinkamai turėjo daugiau išteklių, taigi ruošdamas bylą inspektorius turėjo elgtis labai atsargiai ir dėmesingai, kad išvengtų nemalonumų teisme.

Policininkai, kaip ir dera, rinko įkalčius, o Keithas Mularskis ir Cha0 vis dar bičiuliavosi kaip Tamsiosios rinkos administratoriai. Operacija tęsėsi ištisus penkis mėnesius, ir Bilalas diena iš dienos po trupinėlį kaupė įrodymus. Jis įsitikino, kad Çağatay'aus artimųjų grupė yra palyginti maža, o jo apsauga savo preciziškumu prilygsta karinei. Tačiau, be šių įrodymų, kurie galėjo sieti Çağatay'ų su bet kokiu nusikaltimu, Bilalui rūpėjo dar vienas dalykas: jis vis dar mėgino nustatyti, ar Çağatay'us turi kokį nors bendrininką, kuriuo pasikliauna, ir meldėsi, kad šis tokio neturėtų.

Rugpjūčio pabaigoje Çağatay'us dingo. Jo persekiotojų komandoje kilo panika. Vis dėlto „Haber 7" žurnalistas ir toliau gaudavo žinutes – ne nuo Cha0, bet nuo kažkokio veikėjo slapyvardžiu Yarris, kuris, regis, buvo artimai susipažinęs su Cha0 veikla. Bilalo laimei, Cha0 pasirodė Stambule taip pat netikėtai, kaip ir buvo pradingęs. Šiaip ar taip, tai buvo perspėjimas, kad situacija pavojinga, taigi Bilalas nusprendė rugsėjo mėnesį pereiti prie veiksmų.

Sugrįžę į vilą Tuzloje, įtariamojo persekiotojai nustatė, kad vienas iš jos gyventojų maždaug kas keletą dienų išeina parnešti maisto produktų. Rugsėjo aštuntąją jis ir vėl išėjo. Bilalas Şenas buvo grįžęs į Ankarą ir nerado sau vietos, kai pastatą apsupęs greitojo reagavimo būrys kas minutę telefonu pranešinėjo jam visas naujienas. O tada, kai vyriškis, išėjęs apsipirkti, sugrįžo, jie staiga puolė – įsiveržė į vilą ir prispaudė prie grindų kitus keturis vyrukus. Visur aplink juos patalpose buvo nesuskaičiuojama daugybė kompiuterių ir dešimtys nelegalių skaitytuvų, pusgaminių, „PIN Pad", pardavimo punktų terminalų ir daugybė grynųjų. Reidas baigėsi triumfu – niekas nebuvo sužeistas, o visi įtariamieji buvo suimti.

Keista, bet, pasak *Wired* žurnalo pranešimų, Cha0 arešto buvo laukiama keliomis dienomis anksčiau, po to, kai kažkas iš rašančiųjų į šį žurnalą *Wired* interneto svetainėje paskelbė apie „DarkMarket“. Vienas pabaigoje esantis komentaras buvo parašytas žmogaus, teigiančio, neva jis yra Tamsiosios rinkos administratorius Lordas Cyrikas. Komentaro autorius tvirtino turįs tiesioginių ryšių su Cha0. Ir paslaptingai pridėjo, jog kai kurie iš jo pavaldinių gal ir atsidurs kalėjime, bet Cha0 – niekada.

Ką gi, sudie, Cha0?

35
Tamsiosios rinkos žlugimas

Kad ir kas iš tiesų buvo Cha0, atrodo, kad netikėtas Çağatay'aus Evyapano suėmimas pasėjo paniką tarp jo draugų Tamsiosios rinkos administratorių. 2008 m. rugsėjo 16 d., praėjus mažiau nei savaitei po policijos reido, Meistras Splyntras „DarkMarket" svetainėje paskelbė, kad policijos sėkmė išsekino jo ir jo draugų administratorių nervus. Tai esą apsunkina galimybę jiems ir toliau prisiimti atsakomybę:

> Akivaizdu, jog šis forumas... pritraukia per daug įvairių pasaulinių tarnybų (FTB, Slaptosios tarnybos ir Interpolo) agentų dėmesio. Manau, jog atėjo laikas, kai taip turėjo įvykti. Tenka labai apgailestauti, kad mes atsidūrėme šioje situacijoje, kadangi... mes įkūrėme Tamsiąją rinką kaip pagrindinį anglakalbių forumą verslui vykdyti. Toks gyvenimas. Kai pasiekiate aukštumas, žmonės būtinai pasistengs jus numesti žemyn.

Per savaitę pagrindinė anglakalbių pasaulio kriminalinė svetainė mirė. Jos gerbėjai kraustėsi iš proto. „Tamsioji rinka buvo mūsų tiltas į verslą, ir jei šis tiltas sugriuvo... – sielojosi narys slapyvardžiu Iceburg *Wired* žurnalo interneto svetainėje. – Tegyvuoja pinigų

išgryninimas ir kardingas. Tepražūva visos ŽIURKĖS ir FTB, ir visi kvaili slaptieji agentai, kurie ne tik griauna mūsų gyvenimus ir šeimas, bet ir naikina viską, ką mes sukūrėme."

Atrodė, kad kibernetinė policija laimėjo. Nors Tamsiosios rinkos istorija nebuvo tokia paprasta.

IV dalis

36
Dvigubas pavojus

Štutgartas, 2007 m. rugsėjis

Pareigūnas Dietmaras Lingelis buvo patenkintas savo darbu. Prieš savaitę viršininkas perdavė jam Kanados internetinio pašto paslaugos teikėjo „hushmail" registracijos žurnalus. Ši elektroninio pašto sistema buvo laikoma visiškai neprieinama – niekas negalėjo perskaityti jūsų korespondencijos, jei naudojotės „hushmail" paslauga. Ilgą laiką tai buvo tiesa, bet 2007 m. kompanija pasidavė Kanados policijos spaudimui ir leido policininkams prieiti prie registracijos žurnalų įrašų. Jie atskleidė tyrėjams, kurie IP adresai priskirti tam tikriems elektroninio pašto adresams. Ir Kanados karališkoji raitoji policija perdavė FTB agentui Mularskiui dvi elektroninio pašto adresų paskyras: auto432221@hushmail.com ir auto496064@hushmail.com.

Dar 2007 m. gegužę Matrica buvo atsiuntęs Keithui Mularskiui redaguotą anoniminio elektroninio laiško versiją, kuriame jis buvo perspėtas, kad yra sekamas vokiečių policijos. Pirmiausia Mularskis pamanė, kad už informacijos nutekėjimą atsakingi jo kolegos iš JAV slaptosios tarnybos. Tuo metu Federalinio tyrimų biuro pareigūnai ir Slaptoji tarnyba konkuruodami tarpusavyje atliko

operacijas prieš Tamsiąją rinką ir taip smarkiai padidino galimybę atsirasti saugumo spragoms tiek dėl nekompetentingumo, tiek dėl piktų kėslų. Tačiau bent trijų užsienio šalių policijos pajėgos žinojo apie Matricą: britai, prancūzai ir, suprantama, vokiečiai.

Visi policijoje į elektroninius laiškus žiūrėjo rimtai. Čia galėjo veikti šnipas, bet buvo ir kita ne mažiau nerimo kelianti versija, jog kažkas įsilaužė į kuriam nors tyrimo skyriui priklausančius kompiuterius. Operacijos „DarkMarket" buvo imtasi labai rimtai, bet policijos reidai prieš Matricą ir JiLsi buvo tik pradžia – pagal planą operacija turėjo tęstis kelerius metus. Šis elektroninis laiškas sukėlė pavojų visai strategijai, sukurtai per dvejus kruopštaus darbo metus. Informacijos nutekėjimą reikėjo sustabdyti. Poreikis rasti nutekėjimo šaltinį tapo pagrindiniu tarptautinio tyrimo prioritetu.

Kai „hushmail" elektroninės pašto tarnybos registracijos žurnalai atsirado ant Lingelio darbo stalo, buvo galima pradėti kruopščiai nagrinėti įrodymus. Lingelis, kaip komandos, tiriančios Matricos atvejį, techninis specialistas, turėjo nustatyti, kas mėgino kreiptis šiais elektroninio pašto adresais maždaug tuo metu, kai jie buvo perduoti Matricai.

Lingelis nustatė, kad vienas IP adresas, iš kurio buvo bandoma pasiekti anoniminius elektroninio pašto adresus, buvo iš Štutgarto srities. Jį iš karto atmetė – jis buvo jo paties. Kai Keithas Mularskis pirmą sykį įspėjo Štutgarto policiją apie minėtų elektroninių adresų egzistavimą, Lingelis mėgino įeiti į „hushmail" elektroninį paštą, registruodamasis kokiu nors standartiniu slapyvardžiu (pvz., „admin" ar „password") ir kitais, priklausančiais svarbiausiems Tamsiosios rinkos nariams ir žinomais teisėsaugai. Taip pat jis bandė prisiregistruoti iš IP adresų, esančių Berlyne ar kur kitur Vokietijoje. Rugsėjo dvyliktosios ryte Lingelis, diskutuodamas su savo skyriaus viršininku Gertu Wolfu, paaiškino, kad jie dar neturi įtariamojo, bet jiems pavyko susiaurinti galimų įtariamųjų sąrašą.

Po priešpiečių Wolfas įkišo galvą pro Lingelio duris ir pasakė, kad juodu turi susitikti su savo padalinio viršininku. Lingelis įėjo į kambarį ir pamatė jo laukiančią vyresniųjų policininkų grupę, tarp kurių buvo ir pareigūnas iš bloga lemiančio Štutgarto policijos Vidaus tyrimų skyriaus „Dezernat 3.5“. Lingelis suglumo ir pradėjo nervintis. Pareigūnas staiga paskelbė: „Pone Lingeli, mes pradėsime tyrimą prieš jus, nes manome, kad jūs informavote įtariamąjį, jog jis yra sekamas.“

Lingelis neteko žado. Galiausiai šoką pakeitė pyktis. „Aš lyg kvailys, – pamanė jis, – visą savaitę dirbau su savo bosu narpliodamas šitą painiavą, o tada vieną dieną po priešpiečių jis įkiša galvą pro duris ir suvaro peilį tiesiai man į nugarą.“

„Klausykit, pone Lingeli, – kalbėjo pareigūnas, – jūs turite dvi galimybes. Arba jūs bendradarbiaujate su mumis šiame tyrime, arba mes nedelsdami sodiname jus į kalėjimą kardomajam kalinimui.“

Lingelis sutiko bendradarbiauti. Viršininkas jam paaiškino, kad dabar jis turi pasiimti visas jam likusias atostogas, o paskui bus laikinai nušalintas nuo pareigų iki tolesnio pranešimo.

Maždaug keturiasdešimt penkerių Lingelis turėjo neįprastą praeitį. Jis gimė Namibijos sostinėje Vindhuke, kuri kolonijiniu laikotarpiu buvo vienas iš kelių imperinės Vokietijos Pietvakarių Afrikos kolonijų administracinių centrų. Būdamas penkerių jis su tėvais persikėlė į Keiptauną, taigi užaugęs puikiai kalbėjo tiek angliškai, tiek vokiškai. Jis grįžo į tėvų gimtinę studijuoti, o baigęs įsidarbino policijoje. Čia sparčiai kilo karjeros laiptais kelių policijoje, nors darbas jį ne itin viliojo.

Kaip aistringas kompiuterių mėgėjas, 2001 m. jis pasinaudojo proga ir paprašė būti paskirtas į postą Badeno-Viurtenbergo policijoje. Štutgarto vyriausiajai valdybai reikėjo žmogaus, turinčio darbo patirties su atviro kodo operacine sistema „Linux“, leidžiančia užtikrinti tinklo saugumą. Po penkerių metų, atsižvelgiant į jo, kaip

kompiuterininko, įgūdžius, Lingelis buvo paskirtas į Kriminalinių tyrimų skyrių, kuriam vadovavo Frankas Eissmannas.

Matrica buvo ne vienintelis vokietis, kurį kaip aktyvų Tamsiosios rinkos narį išaiškino Keithas Mularskis. Kiti du buvo Soulfly* (tikrasis vardas Michaelis Artamonovas) ir Fake** (tikrasis vardas Bilge Ulusoy). Iš pradžių valstybės prokuroras norėjo pareikšti Matricai kaltinimą dėl nusikalstamo susivienijimo suformavimo, bet tam reikėjo įrodymų, kad jis bendradarbiavo su kitais dviem sąmokslininkais.

Tačiau dėl kažkokių priežasčių jokie tyrimai prieš Fake ir Soulfly taip niekada ir nebuvo pradėti, o 2007 m. spalį iš dalies dėl teisėjo spaudimo valstybės prokuroras atmetė kaltinimus dėl susivienijimo suformavimo ir pakeitė juos lengvesniais kaltinimais dėl sukčiavimo su kreditinėmis kortelėmis. Klausimas, kodėl jie atsisakė tyrimo dėl įtarimo bendrininkavimu, buvo tik pirmas iš kelių neatsakytų klausimų, galinčių pakirsti pasitikėjimą Vokietijos vietinės ir federalinės policijos sugebėjimais ištirti šią bylą.

O Badeno-Viurtenbergo policija Štutgarte dėjo daug vilčių į Matricos tyrimą. Paprastai visas bendravimas tokiose kaip ši tarptautinėse bylose pereidavo per Vysbadeną, bet vyriausiasis tyrėjas Frankas Eissmannas įtikino savo vyresnybę, kad jam būtų leista tiesiogiai kalbėtis su pagrindiniu žmogumi iš FTB Keithu Mularskiu.

Todėl visi taip smarkiai susierzino, kai Mularskis iš vokiečių programišiaus Matricos sužinojo, kad šis gavo pranešimą iš anoniminio „hushmail" elektroninio pašto adreso, įspėjantį, jog prieš jį ruošiamas policijos reidas. O policija Londone, Pitsburge ir Štutgarte meldėsi, kad šios informacijos šaltinis nebūtų per daug arti jų namų.

* Sielos skrydis. (Angl.)
** Klastotė, falsifikatas; apsimetėlis. (Angl.)

Sulaikę Lingelį tyrėjai pajuto palengvėjimą – atrodė, lyg būtų neutralizavę savo žmogų. Tačiau 2007 m. gruodį „Dezernat 3.5“ atsiuntė Lingeliui laišką, kuriame buvo sakoma, kad nėra naujų įrodymų, siejančių jį su elektroninio pašto pažeidimais, ir kad nuo kito mėnesio, 2008 m. pradžioje, jis gali grįžti į darbą. Visgi jis negrįžo į IV skyrių, tiriantį Matricos veiklą. Lingelis buvo labai pasipiktinęs savo tiesioginiu viršininku Franku Eissmannu, kuris iš dalies buvo atsakingas už tai, kad į jo pavaldinį buvo nukreiptas kaltinantis pirštas.

Vėlyvą pavasarį turėjo įvykti Matricos teismo procesas, ir jam artėjant atmosfera Štutgarto policijos būstinėje buvo niūri ir persmelkta nesantaikos. Negalėdama pareikšti Matricai kaltinimų dėl sąmokslo organizavimo, kaltinančioji šalis suprato, jog vargu ar gali tikėtis nuosprendžio, numatančio laisvės atėmimą. Dar daugiau, jie nė kiek nepajudėjo iš vietos, mėgindami išsiaiškinti, kas nutekino informaciją.

Nors Lingelis buvo pasipiktinęs dėl to, kas jam nutiko, naujas paskyrimas į I skyrių pasirodė jam visai priimtinas, o naujųjų kolegų elgesys su juo buvo pavyzdinis. Po ilgų įtaraus stebėjimo mėnesių jis jautė palengvėjimą ir džiaugėsi pokyčiais.

Tada, 2008 m. gegužę, Lingelis vėl buvo suimtas. Bet šį sykį jis nebuvo kaltinamas rašęs elektronines žinutes Matricai. Lingelis buvo kaltinamas pastatęs į pavojų FTB agento Keitho J. Mularskio slaptąją tapatybę.

37
Zoro nuplėšta kauke

2008 m. birželį, kai buvo teisiamas Matrica, radijo korespondentas Kai'us Laufenas, sklaidydamas Masačusetso technologijų institute išleistą *Technologijų apžvalgos* egzempliorių, pastebėjo straipsnį apie kibernetinius nusikaltimus. Iki tos akimirkos tiriamosios žurnalistikos specialistas iš Vokietijos pietvakariuose esančio Karlsrūhės miesto nė nenumanė, kad šie nusikaltimai tampa tokia rimta problema. Straipsnis jį sudomino, ir jis nusprendė išsiaiškinti, kokiu mastu kibernetiniai nusikaltimai yra paveikę Vokietiją.

Apdairus ir kruopštus Laufenas pradėjo ieškoti Vokietijos baudžiamojo kodekso straipsnių, susijusių su kompiuteriniais nusikaltimais. Juos suradęs išsiuntinėjo elektroninius laiškus į maždaug penkiasdešimt apskričių ir savivaldybių teismų visoje šalyje, klausdamas, ar jiems yra tekę turėti reikalų su šios rūšies bylomis.

Jis gavo tik porą atsakymų, tačiau vienas iš jų Laufeną sudomino, mat jame buvo kalbama apie sukčiavimo su kreditinėmis kortelėmis bylą Badeno-Viurtenbergo užkampio Gepingeno vietiniame teisme, visai netoli nuo tos vietos, kur gyveno Laufenas. Jaunas vyriškis Detlefas Hartmannas laukė nuosprendžio dėl trylikos kaltinimų už klonuotų kreditinių kortelių panaudojimą.

Istorija neatrodė itin įdomi, bet Laufenas visgi nusprendė susisiekti su Štutgarto regiono policija, ir netrukus inspektorius Frankas Eissmannas jau aiškino jam esmines šio kibernetinio nusikaltimo detales. Tarp kitko, jis pasakė, kad jo vadovaujamam IV skyriui tirti Hartmanno bylą padėjo FTB.

Liepos 2 d. Detlefui buvo paskirta devyniolikos mėnesių lygtinė bausmė, o kitą dieną Kai'us parašė jam, prašydamas interviu, ir šį prašymą, nors ir keista, nusiuntė paprastu, o ne elektroniniu paštu. Keli pirmieji žurnalisto mėginimai pasikalbėti su Detlefu ir jo tėvais nepavyko dėl jų pasipriešinimo, bet po trijų mėnesių jie nusileido, taigi spalio pradžioje Kai'us jau sėdėjo priešais jaunuolį prie kavos puodelio.

Kai'us Laufenas nebuvo geltonsnapis. Gimęs šiaurės Vokietijoje, kurį laiką jis augo Brazilijoje ir laisvai kalbėjo portugališkai, ispaniškai ir angliškai. Jam teko dirbti įvairiose Pietų Amerikos vietose, ir jis išmanė apie organizuotą nusikalstamumą ir gangsterius. Tačiau dabar jis vargiai galėjo patikėti savo ausimis, kai Detlefas linksmino jį pasakojimu apie Matricą ir jo nuotykius virtualiame pasaulyje, kur jie visi – šiek tiek gangsteriai, šiek tiek anarchistai ir šiek tiek Tolkienai – didžiavosi ypatingais vardais, o pirkdami ir parduodami vogtus finansinius duomenis bendravo hibridine anglų kalba.

Kai'us be vargo perprato šių naujoviškų piktadarybių prasmę. Naudodamiesi internetu nusikaltėliai galėjo vykdyti nusikaltimus prieš daugybę už tūkstančių mylių esančių nežinomų aukų, kurios gal suprasdavo, o gal ir ne, kad jų privatumas pažeistas, o pinigai ar tapatybės duomenys vagiami.

Vis dėlto, svarstė Kai'us, jeigu tai šitaip paprasta, kodėl Detlefas buvo suimtas? „Nieko ypatingo, – atsakė šis, – vienas iš mano bičiulių administratorių, su kuriuo aš daugelį mėnesių dirbau, buvo FTB agentas. Jis sekė mane ir įspėjo Vokietijos policiją." Žurnalistas pamanė, kad galbūt jaunuolis per daug susireikšmina, taigi paklausė, ar jis turi kokių nors dokumentinių įrodymų šiam teiginiui paremti. „Taip, – atsakė Detlefas, – aš jums juos atsiųsiu."

Po kelių dienų Detlefas atsiuntė Laufenui prokuroro pareiškimą, bendrais bruožais nusakantį valstybės bylą prieš jauną žmogų ir parašytą neprilygstama teisine vokiečių kalba:

> Remiantis tyrimo dokumentais, šis administratorius, kuris pagal galutinį bylos nagrinėjimą visiškai kontroliavo visus susitarimus bent jau nuo 2006 m. birželio mėn. ir vėliau, yra FTB agentas Keithas Mularskis, kuris pasiūlė serverio prieglobą, kad būtų galima surinkti tikslesnę informaciją apie pirkėjus ir pardavėjus. Čia aš remiuosi bylos dokumentu Nr. 148, aplankas I, kuriame Keithas Mularskis taip informuoja tyrėją pareigūną Franką Eissmanną [*sic*]: *Meistras Splyntras* [sic] *esu aš.* Kad naudotojas Meistras Splyntras valdė serverį, įrodo bylos dokumentas Nr. 190 ir 2007-03-09 elektroninis laiškas iš Keitho Mularskio: *Jis man sumokėjo už serverį.*

Kai'us buvo apstulbęs. Jis iš naujo perskaitė pagrindinį sakinį. *Meistras Splyntras esu aš.* Negana, kad Detlefas Hartmannas buvo teisus, sakydamas, jog jo kibernetinius darbelius seka FTB, bet dar ir prokuroro tarnyba įvardijo agentą *ir* jo slapyvardį. Žaidimas tęsėsi, o jis, Kai'us Laufenas, atskleidė tiesą apie vieną iš svarbiausių pasaulio kibernetinių policininkų. Prieš tris mėnesius jis vargu ar iš viso buvo girdėjęs apie kibernetinius nusikaltimus.

Kai Kai'us paskambino į Mokymų apie kibernetinių nusikaltimų įrodymus nacionalinį aljansą Pitsburge, jį iš karto sujungė su Keithu Mularskiu, ir šis, kaip visada, kuo maloniausiai bendravo. Bet kai žurnalistas perskaitė sakinį iš elektroninio laiško: „Meistras Splyntras esu aš“, – kitame linijos gale stojo mirtina tyla. Keithas suprato, jog įkliuvo. Gera žinia buvo ta, kad jį pričiupo ne kas kitas, o radijo žurnalistas iš pietvakarių Vokietijos, ir net šiame interneto amžiuje egzistavo labai nedidelė tikimybė, kad žinia nepasklis daug toliau už Badeno-Viurtenbergo ribų. Nors širdyje jis nujautė, kad ta tikimybė tikrai labai menka.

Ar tai vėl tas nelemtas informacijos nutekėjimas?

Kai'us Laufenas nežinojo, kad Štutgarto policijos komisaras antrą kartą sankcionavo Dietmaro Lingelio nušalinimą nuo pareigų. Tačiau šį sykį buvo įtariama, jog pareigūnas tyčia perdavė Mularskio pavardę ir slapyvardį prokurorui, kad šis galėtų juos įtraukti į savo bylos metmenis. Buvo įtariama, jog Lingelis siekė iškelti į viešumą Mularskio tapatybės duomenis ir kartu diskredituoti FTB. Motyvacija, kaip teigė komisaras, buvo Lingelio nepasitenkinimas kai kuriais policijos veikimo metodais, panaudotais tiriant Hartmanno bylą.

Lingeliui pareikšti įtarimai padėjo išryškinti fundamentalius teisėsaugos filosofijų Europoje ir Jungtinėse Valstijose skirtumus. Europiečiai linkę vengti operacijų su policijos paspęstomis pinklėmis, nes laiko jas rizikingomis ir moraliai bei teisiškai abejotinomis. Amerikiečiai, priešingai, dažnai tuo naudojasi. Amerikoje vyksta intensyvūs debatai dėl to, kur baigiasi policijos pinklės ir prasideda provokavimas. Europoje kai kurie policijos pareigūnai manė, kad Tamsiosios rinkos operacija balansuoja ant rizikingos bedugnės krašto, kadangi būtent Slaptoji tarnyba, atrodo, ypač skatino savo narius tyrimo metu dalyvauti kriminalinėje veikloje (pavyzdžiui, Drono atveju). FTB ir Keithas Mularskis energingai gynė savo veiksmus, pabrėždami, jog Mularskio ir jo komandos dalyvavimas Tamsiojoje rinkoje suteikė galimybę rinkti informaciją – ypač apie Cha0 ketinimą išplėsti operacijas Jungtinėse Valstijose, o tai, Mularskio tvirtinimu, neleido prarasti apie 70 milijonų JAV dolerių.

Tuo metu, kai Kai'us Laufenas dėliojo paskutinius štrichus savo radijo laidai apie šią specifinę, tačiau svarbią istoriją, jis pajuto skausmą, kurį sukėlė disko išvarža. Beveik visiškai negalėdamas pajudėti, žurnalistas buvo priverstas dvi savaites pragulėti lovoje. Jis padarė išvadą, jog niekam Vokietijoje nerūpi tas faktas, kad FTB sulaikė vokiečių karderį ir kad jis, Kai'us, atskleidė agento tapatybę. Iš kitos pusės, Tamsiosios rinkos istorija sulaukė didelio su technologijomis

susijusios JAV žiniasklaidos dėmesio. Parodžius iniciatyvą San Fransiske leidžiamam žurnalui *Wired*, šia tema buvo paskelbta nemažai informacijos, ypač po dramatiško Merto Ortaço pagrobimo tų metų balandžio mėnesį ir Cha0 arešto rugsėjo mėnesį.

Kai'us tvirtai tikėjo, kad turi išplatinti įrodymus, jog Tamsioji rinka iš dalies yra operacija su FTB paspęstomis pinklėmis. Tačiau kaip abipus Atlanto skiriasi policijos darbo kultūra, lygiai taip skiriasi ir vokiečių ir jų anglų bei amerikiečių kolegų žurnalistinės etikos standartai. (Britanijos policija yra europietiška, o ne amerikietiška, tačiau Britanijos žiniasklaida turi netgi mažiau skrupulų nei amerikiečiai.)

Vokietijoje laikoma blogu tonu publikuoti įtariamų nusikaltėlių vardus ir pavardes tol, kol jie teisiami, ir daugeliu atvejų Vokietijos žiniasklaida nedaro to netgi vėliau, kai nusikaltėliai pripažįstami kaltais. Tas pats pasakytina ir apie slaptuosius policijos agentus. Bet kam, susipažinusiam su anglų ir amerikiečių žiniasklaida, toks požiūris yra nesuvokiamas.

Taigi kai Kai'us Laufenas 2008 m. spalio pradžioje telefonu kalbėjosi su *Wired* žurnalo redaktoriumi saugumo klausimais Kevinu Poulsenu, jis pasakė, jog pateiks ponui Poulsenui dokumentinius įrodymus, patvirtinančius, kad teisėsauga įsiskverbė į Tamsiąją rinką. Jis pridės Keitho Mularskio prisipažinimą elektroniniu paštu apie jo, kaip Meistro Splyntro, vaidmenį, bet tik su griežta sąlyga, kad Poulsenas nepaskelbs Mularskio pavardės. Pakartojęs šį teiginį, savo elektroninį laišką, prie kurio buvo pridėti nuskenuoti dokumentai, Laufenas baigė tokiu pamokymu: „Perskaitęs sunaikinkite!"

Poulsenas tai prisimena kiek kitaip: jis tik sutiko neskelbti spaudoje tikrojo Matricos vardo. Per kelerius metus jis su savo komanda atliko įspūdingą darbą, atsekdamas daugumą kibernetinių nusikaltimų istorijų, tarp jų ir Tamsiosios rinkos istoriją. Iš tiesų jis dirbo taip pat uoliai, kaip ir anksčiau, būdamas programišiumi,

nors ši jo karjera baigėsi kriminaliniu kaltinimu. Taigi perskaitęs laišką Poulsenas jo nesunaikino. Pirmadienį, spalio mėn. 13 d., jį paskelbė. Meistras Splyntras mirė.

Savo ruožtu Keithas Mularskis įsiuto, kai *Wired* paskelbė jo vardą – pasitikėjimas, kurį jis buvo užsitarnavęs tarp daugelio karderių, buvo prarastas akimirksniu. Prieš porą savaičių jis buvo uždaręs Tamsiosios rinkos forumą, nes JiLsi įregistruoto domeno vardo galiojimo laikas greitai turėjo baigtis. Jei Meistras Splyntras būtų mėginęs jį perregistruoti, koks nors smalsus programišius būtų galėjęs pasinaudoti proga ir atskleisti jo tapatybę.

Tamsiosios rinkos operacija buvo ilgalaikio teisėsaugos plano prasiskverbti į kibernetinių nusikaltimų pasaulį pirmasis etapas. Per penkiolika mėnesių, anksčiau nei *Wired* žurnale buvo paskelbta Mularskio pavardė, FTB, Sunkių organizuotų nusikaltimų agentūra SOCA ir kitos su šiais reikalais susijusios policijos tarnybos, kruopščiai dirbdamos, tai vienur, tai kitur buvo sulaikiusios pavienius asmenis. Šios tarnybos buvo sąmoningai nusprendusios nepradėti „šluoti“ „DarkMarket“ narių plačiu mastu, priešingai tai taktikai, kurią 2004 m. Slaptoji tarnyba panaudojo, susidorodama su „Shadowcrew“. Meistras Splyntras rimtai ketino sugrįžti sutvirtinęs savo reputaciją ir apsiginklavęs didele karderių ir jų veiklos duomenų baze. Dabar šis planas netikėtai žlugo.

Nepasakytum, kad Mularskio pastangos buvo bergždžios – tai buvo puikus tarpvalstybinio bendradarbiavimo tarp skirtingų policijos struktūrų pavyzdys, kai buvo sugauta viena iš didžiausių kardingo pasaulio žuvų Cha0 ir suimti dešimtys kitų, kai kurie iš jų jau buvo nuteisti, o dauguma dar laukė teismo.

Bet nei Mularskis, nei kas nors kitas negalėjo apkaltinti Dietmaro Lingelio. Ne jo leidimu Meistro Splyntro tapatybė praslydo į teismo dokumentus Matricos byloje, kaip buvo įtaręs pareigūnas iš „Dezernat 3.5“.

Šiuo atveju „pasižymėjo" Lingelio viršininkas detektyvas Frankas Eissmannas. Vėliau jis prisipažino, jog „padarė didelę klaidą", kartu su kitais policijos parodymais prieš Matricą pateikdamas valstybės prokurorui ir šį dokumentą. Eissmanno klaida privedė prie to, kad Kai'us Laufenas atpažino Mularskį, o tai sužlugdė ilgalaikę operaciją prieš karderius.

Visgi Dietmaras Lingelis tebebuvo nušalintas nuo pareigų ir negirdėjo jokių žinių iš savo bendradarbių iki tol, kol 2010 m. rugsėjį „Dezernat 3.5" pranešė, kad jam teks stoti prieš teismą. Prokuroras atmetė nepagrįstą pareiškimą, kad Lingelis sąmoningai nutekinęs Mularskio pavardę. Vietoj to buvo atgaivintas pirmasis kaltinimas: neva jis pranešęs įtariamajam, jog šis yra sekamas.

Lingelis nusprendė užginčyti kaltinimus, taigi vėliau tą patį mėnesį Štutgarte prasidėjo pats ilgiausias kada nors įvykęs teismo procesas, susijęs su Tamsiosios rinkos byla. Ironiška, jog į jį nebuvo įtraukti jokie tikrieji kibernetiniai nusikaltėliai (išskyrus tai, kad Matrica ir Fake davė parodymus kaip liudytojai), o tik Badeno-Viurtenbergo policija kovojo su vienu savo pačios pareigūnu. Tai buvo žavus reginys, suvaidintas saujelės žmonių akivaizdoje švariame, mažame beveidžiame teisme Bad Kanštate, Štutgarto mineralinių vandenų kurortų rajone. Beveik tuzino dramos veikėjų parodymai buvo pritrenkiantys, nes atskleidė daugelį klaidų ir nesėkmių, nukamavusių policijos operacijos dalyvius tiek Europoje, tiek Jungtinėse Valstijose.

38
Kas tu toks?

Stambulas, 2008 m. spalis

Çağatay'us Evyapanas kalėjime atrodė atsipalaidavęs. Retkarčiais koks nors Stambulo policininkas pašnibždėdavo ką nors apie svarbų pareigūną, atskrendantį iš Ankaros į pagrindinį Çağatay'aus tardymą. Turkijoje asmenį, įtariamą dalyvavus organizuotoje nusikalstamoje veikloje, ilgiausiai galima sulaikyti keturioms paroms. Kaliniui buvo smalsu įsitikinti, ar tas misteris Didelis Žmogus iš sostinės pasirodys.

Galiausiai atvyko inspektorius Şenas. Jam rūpėjo išsiaiškinti tik vieną dalyką.

– Kas tas nenaudėlis? Su kuo tu kalbiesi? Tai viskas, ką noriu iš tavęs sužinoti.

Kalinys padvejojo. Tada jo veide pasirodė neviltis.

– Ten nieko nėra.

39
Kelyje į niekur

Inspektoriaus Şeno darbas buvo baigtas. Kaip reikalauja Turkijos įstatymai, po arešto byla buvo perduota prokuroro tarnybai. Bet jei Çağatay'us Evyapanas yra Cha0, tai kas per veikėjas yra Şahinas, kuris, Merto Ortaço teigimu, ir yra tikrasis Cha0? Ar Şahinas – tai tik Merto vaizduotės padarinys? Šiaip ar taip, Mertas buvo žinomas kaip fantazuotojas ir mėgėjas viską sureikšminti.

Nors Mertas ir labai mėgo suraizgyti pasakojimo siūlus, esminiai jo pasakojimo aspektai buvo teisingi. Jis iš tiesų dirbo įvairioms oficialioms organizacijoms, įskaitant ir Žvalgybos tarnybą; jis buvo labai talentingas programuotojas, itin įgudęs šifruoti lustines korteles; jis uždirbo milžiniškas sumas pinigų, pardavinėdamas „Digiturk" korteles, ir vėliau buvo dėl jų tardomas; jis švaistė pinigus pramogoms ir žmonėms, kuriems norėjo padaryti įspūdį; jis reiškėsi Tamsiosios rinkos forumuose, naudodamasis ir Saduno slapyvardžiais Cryptos ir PilotM; jis atostogavo su savo mergina „Adam & Eve" viešbutyje Antalijoje; ir jis neabejotinai buvo pagrobtas ir pažemintas Çağatay'aus Evyapano.

Vis dėlto jis negalėjo pateikti jokių įrodymų, kurie pagrįstų jo pagrindinį teiginį, kad po Cha0 slapyvardžiu iš tiesų slėpėsi paslaptingasis Şahinas. Tačiau Mertas demonstravo tokias išsamias žinias apie Tamsiosios rinkos vidinį funkcionavimą, jog atrodė, kad kalba tiesą iš savo patirties, nebent kai kurias ar visas šias detales būtų sužinojęs iš kokio nors asmens ar organizacijos. Klausimas išlieka –

ir, beje, nė iš tolo neatsakytas – kodėl? Ir ką norima apšmeižti ar diskredituoti, sviedžiant į šią maišalynę nepaprastąjį poną Ortaçą? Tikrai ne Çağatay'ų Evyapaną, nes Merto istorijoje jis yra menkesnis nusikaltėlis. Policiją? O gal žmogų, kuris, Merto teigimu, buvo iškilus Turkijos ir globalinės internetinės scenos veikėjas ir vadinosi Lordu Cyriku?

Visgi Merto tiesa išlieka ne mažiau tikėtina nei inspektoriaus Şeno. Esmė ne Şahino ar Çağatay'aus asmenybė. Esmė – pats Cha0 personažas. Nėra abejonių, kad žmogus, sugalvojęs ir įkūręs kreditinių kortelių duomenų nuskaitymo prietaisų fabriką ir vykdęs Tamsiosios rinkos administratoriaus pareigas, buvo Çağatay'us Evyapanas. Kyla klausimas, ar Evyapanas vadovavo visai operacijai, ar tik dirbo stambesnio kriminalinio sindikato naudai.

Apskritai Turkijos policija suėmė kiek daugiau nei porą dešimčių žmonių, kurie, kaip teigiama parodymuose, buvo Cha0 vykdomos operacijos arba artimiausia aplinka, arba antraeiliai veikėjai. Toks jau yra virtualus nusikaltėlis – tai nėra vienas realus veikėjas, bet atskirų individų, turinčių įvairių įgūdžių, junginys, dirbantis kaip atskiras vienetas. Lygiai taip ukrainietis „CarderPlanet" įkūrėjas Skriptas pripažino, jog po bendru pavadinimu „karderis" iš tiesų slepiasi daugybė įvairių gebėjimų: kai kurie karderiai buvo tikrieji įsilaužėliai; kai kurie – grafikos dizaineriai; kiti – elektronikos specialistai, kuriantys nelegalius skaitytuvus; kai kurie nuskaitydavo informaciją iš bankomatų; kiti grynindavo pinigus; dar kiti pasirūpindavo saugumu; o kai kurie rinkdavo informaciją: kartais nusikaltėliams, o kartais – policijai.

Taigi abu vyrai – ir Cha0, ir Skriptas – numatė, koks bus kibernetinių nusikaltimų pasaulis po Tamsiosios rinkos: nuo silpnai susisaisčiusios individų, užsiimančių savanaudiška kriminaline veikla, bendruomenės jis pereis prie daug metodiškiau dirbančios kriminalinės organizacijos, kurios nariai atliks specialias užduotis: siuntinės

elektroninį brukalą, kurs virusus, plaus pinigus, naudos kenkėjiškomis programomis užkrėstus kompiuterių tinklus ar užsiims kita svarbia virtualaus pasaulio nusikalstama veikla.

Taigi galbūt Cha0 vardu vadinosi būtent tokia operacija, kurioje visa šutvė veikė išvien. Cha0 buvo kolektyvinis vardas, kuriuo prisidengus visų pirma buvo siekiama užkariauti bent jau dalinę monopoliją naujoje sukčiavimo su kreditinėmis kortelėmis srityje – panaudojant nelegalius kortelių duomenų nuskaitymo įrenginius. Tai buvo rizikingas planas, kuris būtų pasisekęs, jei ne suvienytos Keitho Mularskio ir Bilalo Şeno pastangos ir parama, kurią teikė kitos policijos tarnybos ir tam tikri kiti asmenys.

Tokio subjekto kaip Cha0 organizavimas aiškiai leidžia galvoti kiek kitaip. Tradicinės kriminalinės bendrijos dar visai neseniai „kibernetinius nusikaltėlius buvo linkusios laikyti antrarūšiais piliečiais", kaip juos apibūdino vienas iš vadovaujančiųjų Sunkių organizuotų nusikaltimų agentūros SOCA kibernetinės policijos atstovų. Tačiau Tamsiosios rinkos egzistavimo laikotarpiu viso pasaulio policijos pajėgos vis dažniau pastebėdavo, jog tiriant kibernetinius nusikaltimus paaiškėja, kad čia netikėtai pasirodo tradicinės organizuotų nusikaltėlių grupės.

Pačioje Tamsiojoje rinkoje egzistavo trys gana aiškiai apibrėžtos projekte dalyvaujančios grupės. Pirmajai priklausė administratoriai, moderatoriai ir kiti, einantys svetainėje aukštesnes „biurokratines" pareigas. Daugiausia tai buvo vyrukai, turintys pažangiausių įsilaužimo įgūdžių, ir, be abejonės, puikūs kompiuterių žinovai. Dar daugiau, visi jie, išskyrus Cha0, arba neuždirbdavo didelių pinigų, arba paprasčiausiai dirbo policijos agentais ar slaptais informatoriais.

Be šių vyrukų, buvo antra grupė, iš esmės susidedanti iš įgudusių ir patyrusių nusikaltėlių, kurie daugiausia dirbo savarankiškai; pavyzdžiui, Freddybb ir Raudonoji Brigada. Jie pasižymėjo įvairaus lygio kompiuteriniais įgūdžiais ir, jei patys nesugebėdavo išspręsti

techninių problemų, visada pažinojo žmones, galinčius tai padaryti. Tokiuose forumuose kaip Tamsioji rinka šie asmenys reikšdavosi mažiau nei administratoriai ir jų komanda. Jų tikslas buvo užsidirbti kuo daugiau pinigų, neatkreipiant į save dėmesio, nors jie taip pat kartkartėmis dalyvaudavo smagiuose pasiplepėjimuose ir pokalbiuose apie kardingo bendruomenę kaip visumą.

Trečią grupę sudarė profesionalūs nusikaltėliai, kurių iš esmės nematė ir nežinojo niekas, išskyrus policiją ir jų bičiulius karderius, ir tai tik iš mitų ir atsiliepimų. Tai buvo žmonės, kurie nepriklausė netgi prie kreditinių kortelių ir kenkėjiškų programų pagrindinių didmenininkų – tokie vyrukai kaip ukrainietis Maksikas, kurį Turkijos komanda, kovojanti su kibernetiniais nusikaltimais, suėmė Antalijoje 2007 metais. Įžymiausias iš jų (kuris, kaip manoma, tiekdavo Maksikui daugumą medžiagos) yra rusas, visuotinai žinomas kaip Simas, nors, policijos manymu, iš tiesų tai dar vienas labai produktyvus sindikatas. Tai žmonės, kurie niekada neišlenda iš šešėlio.

Cha0 buvo patrauklus ir svarbus, kadangi tai buvo pirmas atvejis, kai organizuota grupė, panaši į tradicinę organizuotų nusikaltėlių grupuotę, įsitraukė į plataus masto kibernetinius nusikaltimus ir siekė paveikti tokios interneto svetainės kaip „DarkMarket" funkcionavimą. Tai buvo pirmas realus įrodymas, kad kibernetiniai nusikaltimai jau nebėra tik antrarūšių piliečių veiklos sritis – jie ėmė traukti ir kai kurias svarbesnes figūras.

Organizuotas nusikalstamumas Turkijoje tradiciškai yra labai galingas. Pavyzdžiui, kartu su kurdų ir kai kurių kitų Balkanų šalių grupėmis turkų gaujos viešpatauja didmeninėje heroino prekyboje visoje Vakarų Europoje.

1996 m. pabaigoje šarvuotas mersedesas pateko į šiurpų eismo įvykį mažame Susurluko miestelyje. Tarp žuvusiųjų buvo Policijos akademijos viršininkas ir dešinės pakraipos teroristinės grupės lyderis Grey'us Wolvesas, kuris taip pat buvo Interpolo ieškomiausių žmonių

sąraše kaip vienas iš pagrindinių prekiautojų heroinu ir kaip žinomas samdomas žudikas. Vienintelis gyvas išlikęs žmogus buvo parlamento narys iš tuometinės valdančiosios partijos.

Šis įvykis leido žurnalistams ir opozicijos politikams pradėti žiauraus suktybių tinklo, į kurį buvo įsivėlusi Turkijos „valstybė valstybėje" kartu su pačiais įtakingiausiais organizuotų nusikalstamų grupių nariais, išpainiojimą. Metų metais jie naudojosi vieni kitų draugiškumu, svetingumu ir apsauga. Įvairios istorijos ne tik sukrėsdavo eilinius turkus, bet ir suteikė svarbų stimulą Turkijos politikoje atsirasti naujoms jėgoms – pavyzdžiui, organizacijai, galiausiai.tapusiai AK partija, kuriai kova prieš nusikalstamumą ir korupciją tapo pagrindine politinės platformos dalimi.

Nuo tada Turkija šiek tiek pasistūmėjo į priekį. Tačiau kai korupcija ir organizuotas nusikalstamumas įsišaknijęs taip giliai kaip Turkijoje praeito amžiaus devintame ir dešimtame dešimtmečiuose, prireiks kelių dešimtmečių, kol jos bus nukirstos nuo politikos kūno. Tai paaiškina Bilalo Şeno išgąstį pirmą kartą išgirdus, jog Cha0 galbūt gyvena prisiglaudęs po galingų valstybės aparato vyrų sparneliu. Tai labai tikėtina, nes kai kurie Bilalo kolegos iš kitų šalių mano, jog Tamsiojoje rinkoje apsigyvenęs Cha0 priklausė daug didesnei organizacijai. Nusikalstamos grupuotės Turkijoje apima įvairius sektorius – be prekybos heroinu, Turkija yra ir pagrindinis prekybos žmonėmis centras (vėlgi dėl to, jog yra arti Europos Sąjungos šalių). O per du paskutinius dešimtmečius ten išaugo ir pinigų plovimo verslas.

Taigi, pagal jų teoriją, Çağatay'us Evyapanas iš tiesų buvo tik Cha0 holdingo kompanijos vadovo pavaduotojas. Çağatay'us galėjo būti kibernetinių nusikaltimų padalinio viceprezidentas ir sutiko sėsti į kalėjimą, nes, kalbant metaforiškai, „atstatė krūtinę bosui skirtai kulkai". Galbūt visos kompanijos vadovas yra Şahinas. Jei

taip būtų, Şahinas iš Merto pasakojimų gali egzistuoti, bet inspektorius Şenas vis vien bus suėmęs tinkamą žmogų.

Tamsioji rinka buvo uždaryta 2008 m. spalį, tačiau niekas – nei teisėsaugos institucijos, nei patys nusikaltėliai – taip ir nesuprato, kokia buvo jos tikroji istorija ir kokia yra jos tikroji reikšmė. Praėjus trejiems metams tik mažai daliai iš maždaug šimto suimtųjų visame pasaulyje buvo iškeltos baudžiamosios bylos.

Teisinės sistemos itin sunkiai susidoroja su aukšto lygio techninės prigimties kibernetinių nusikaltimų įrodymais, tačiau tie modeliai, pagal kuriuos vykdoma dauguma nusikaltimų trečiosiose šalyse, taip pat sukuria milžiniškus barjerus, kai reikia atskleisti nusikaltimus ir jų kaltininkus patraukti baudžiamojon atsakomybėn. Dviprasmiškumas, abejonės, iliuzijos ir veidmainystė visada vaidino svarbų vaidmenį, mėginant atskleisti organizuoto nusikalstamumo būdus ir priemones. O internetas jų galią sustiprina daug kartų.

40
Vidurdienio ekspresas

Tekirdaho kalėjimas, vakarų Turkija, 2011 m. kovas

Gana dailus vyriškis elegantišku juodu kostiumu ir juodu kaklaraiščiu, įėjęs į mažą pailgą kambarį, tiriamai stebėjo mane. Jis buvo šiek tiek pliktelėjęs, o juodų akių žvilgsnis hipnotizavo, ir aš akimirksnį netekau žado. Tai buvo žmogus, apie kurį aš skaičiau, kalbėjau ir galvojau beveik dvejus metus. Dabar, kai pagaliau jį sutikau, staiga nebesugalvojau, ką tinkamo pasakyti.

Kalėjime jis gal ir veltui praleido dvejus su puse metų, tačiau neprarado nei šaltakraujiškumo, nei rūpestingos savitvardos. Per visas tris mūsų pokalbio valandas aiškiai supratau, jog jis ėmė interviu iš manęs lygiai taip, kaip aš iš jo.

Mano pirmas trumpas apsilankymas Tekirdahe įvyko 1976 m., prieš pat pasirodant knygai *Vidurnakčio ekspresas* (*Midnight Express*), pagal kurią vėliau Alanas Parkeris sukūrė pasisekimo sulaukusį kino filmą. Ten pasakojama jauno amerikiečio Billy Hayeso, sugauto su narkotikų kontrabanda iš Turkijos, istorija. Baisus išmėginimas, kurį jis patyrė, pakliuvęs į sadisto kalėjimo prižiūrėtojo rankas, sukrėtė visus Europos ir Jungtinių Valstijų žiūrovus. Tuo metu Turkija turėjo žiaurios ir neatlaidžios šalies reputaciją. Ir iš tiesų, kai ten buvau, miegantį palapinėje mane užpuolė grupė chuliganų, skanduodami reikalavimą užsieniečiui nešdintis namo.

Po trisdešimt penkerių metų aš atsidūriau Tekirdaho kalėjime. Kaip ir tas kalėjimas, kuriame buvo laikomas Hayesas, jis buvo

įrengtas pagal griežčiausius saugumo reikalavimus. Išsidėstęs maždaug mylios aukštyje ant nuolaidaus šlaito, jis, kiek akys užmato, buvo apsuptas dykviečių. Už storos sniego uždangos pastebėjau išblukusias kreminės spalvos sienas ir stebėjimo bokštelius su sargybą einančių kulkosvaidininkų siluetais. Pirmas įspūdis sukėlė mintį, kad nuo Parkerio filmo laikų niekas nepasikeitė.

Tačiau viduje man palengvėjo sužinojus, kad šioje šalies dalyje bent jau kalėjimai neatpažįstamai pagerėjo. Visi kaliniai kamerose turėjo televizorius, dušus ir tualetus. Maistas buvo gana spartietiškas, bet neabejotinai maistingas ir gana skanus, o sargybiniai elgėsi mandagiai ne tik su manimi, bet ir su kaliniais. Kai kuriais atžvilgiais sąlygos čia buvo geresnės nei daugelyje Britanijos kalėjimų.

Tekirdahe kalėjo keli žinomi nusikaltėliai, tarp jų – armėnų rašytojo Hranto Dinko nužudymo iniciatorius. Rašytoją ekstremistai nužudė vien todėl, kad jis buvo armėnas. Nestebino ir tai, kad kalėjime sėdėjo keli įžymiausi Turkijos narkotikų prekybos šulai.

O tarp teroristų ir mafijos vadeivų čia kalėjo ir moderniausios nusikaltimų formos – kibernetinių nusikaltimų – atstovas. Daugiau nei metus užtruko, kol gavau teisę pasikalbėti su Çağatay'umi Evyapanu: turėjau įtikinti tiek Turkijos valdininkus, tiek ir patį Evyapaną. Ilgus mėnesius tai atrodė visiškai neįmanoma. Mano nuostaba buvo beribė, kai vieną pirmadienį 2011 m. kovo pradžioje iš Ankaros kalėjimų valdybos gavau pranešimą, kad jei Çağatay'us neprieštaraus, man bus leista susitikti su juo tos pačios savaitės trečiadienį. O tada, pasak pranešimo, Çağatay'us bus perkeltas ir siauras mano galimybių langelis užsidarys.

Tačiau Turkijos valdininkai nežinojo, o gal jiems tiesiog nerūpėjo, kad mano pasas giliai įstrigęs Kinijos ambasados Londone konsuliniame skyriuje, nes tvarkiau dokumentus vizai gauti. Mano pastangos atsiimti pasą, kad antradienį galėčiau nuskristi į Stambulą, atsimušė į nepermaldaujamą kinų pareigūnų abejingumą. Taigi

susisiekiau su Tekirdaho kalėjimu tiesiogiai ir maldavau jų leisti atidėti interviu vienai dienai. Man buvo pranešta, kad jei jie gaus orderį perkelti Cha0 iki ketvirtadienio, tada, nepaisant to, ar aš būsiu, ar nebūsiu ten atvykęs, man nebebus leista jo pamatyti. Medžioklė pasibaigs.

Taigi buvau labai sunerimęs, kai diena vėliau, ketvirtadienio ryte, kovodamas su sniego pūga skubėjau iš Stambulo į Tekirdahą. Buvo visai tikėtina, jog atvyksiu tik tam, kad išgirsčiau, jog praradau šansą asmeniškai susitikti su Cha0. Po ilgo laukimo buvau įvestas pro trejus besisukančius storo plieno vartus, kurių mechanizmas užfiksavo mano rankos biometrinį atspaudą, ir supažindintas su kalėjimo direktoriumi. Priešingai, nei buvo galima tikėtis, jis visai nebuvo panašus į pabaisą, o greičiau į žavų ir malonų žmogų. Jis pasakė, kad jie negavo jokių nurodymų iš Ankaros ir kad po priešpiečių valgykloje aš galėsiu pasikalbėti su ponu Evyapanu.

Pagaliau mane nuvedė į mažą pailgą kambarėlį. Çağatay'us Evyapanas man pasirodė atsargus, bet pasitikintis savimi žmogus. Taip, kaip ir buvo sakęs Bilalas Şenas, jis iš karto būtų instinktyviai pajutęs, jei suktais būdais būčiau bandęs iš jo išpešti kokias nors informacijos nuotrupas. Jis man priminė „WikiLeaks" įkūrėją Julianą Assange'ą – nepaprastai protingas, bet ironiškas ir įsitikinęs savo intelektiniu pranašumu, o tai kai kuriais atvejais būtų galima palaikyti aukščiausio laipsnio narcisizmu.

Kai jam užsiminiau, kad Lordas Cyrikas yra Tonis – mažas storulis akiniuotas verslininkas, minėtas Merto Ortaço, – jis suprunkštė su giliausia panieka. „Jūs kalbėjotės su turkų žvalgyba, ar ne?" – kandžiai paklausė. Taip sakydamas Cha0 buvo teisus: jei Mertas melavo (pripažinkime, jog tai įmanoma), vadinasi, akiniuotą vyrą į jo pasakojimą įvedė Turkijos nacionalinės žvalgybos tarnyba MIT.

Tačiau mums besikalbant Çağatay'us patvirtino kai kuriuos labai svarbius Merto istorijos aspektus, tarp jų buto, kuriame buvo

laikomas pagrobtas Mertas, buvimo vietą ir Merto bendravimą su vietinės Amerikos ambasados darbuotoja Lucy Hoover. Jis taip pat pripažino, kad jo suėmimas ir šį sykį įvyko dėl realiame pasaulyje padarytos klaidos.

Nors ir visapusiškai susitvardantis ir protingas, Cha0 prasitarė, jog dėl kai ko smarkiai baiminasi – ironiška, bet tai buvo tas pats neišsakytas nerimas, kuris persekiojo jo priešus iš Turkijos policijos. Jis teigė, kad per apklausą vienas iš jo tardytojų pasiūlė jam suteikti apsaugą, jei mainais jis sutiktų duoti parodymus Ergenekono bylos tyrime. Jie reikalavo, kad jis prisipažintų įkūręs slaptą kibernetinį tinklą, skirtą „valstybei valstybėje" bendrininkauti su kariškiais, žvalgybos tarnybomis ir žiniasklaida. Policija savo ruožtu kategoriškai neigia, kad jam buvo pateiktas toks pasiūlymas.

Cha0 atsisakė – labiausiai jis nenorėtų kaip inspektorius Şenas įsivelti į kovą tarp „valstybės valstybėje" ir vyriausybės. Kibernetinėje erdvėje reikalai tvarkomi kitaip.

Per visą mūsų pokalbį Çağatay'us teigė, kad jis ir nedidelė programišių grupelė daug geriau nei bet kas iš valdžios atstovų suvokia, kas vyksta tamsiojoje interneto pusėje. Jis leido suprasti, kad paprasčiausiai siekė pademonstruoti teisėsaugos ir teisėtvarkos pajėgų pastangų beviltiškumą mėginant kontroliuoti internetą, ir tvirtino, jog visada atsiras tokių kaip jis, kurie pirmaus šiame žaidime.

Stebėtina, bet jis neatrodė išmuštas iš pusiausvyros dėl įkalinimo ir to fakto, kad jam gali tekti atlikti likusią dvidešimt dvejų metų laisvės atėmimo bausmę pagal ankstesnį 2000 m. kaltinamąjį nuosprendį, jau nekalbant apie papildomus kaltinimus, kurie gali būti pateikti dėl jo veiklos Tamsiojoje rinkoje.

Kai prakalbome apie FTB ir Keithą Mularskį, jo veide palengva atsirado triumfuojanti išraiška. „FTB nieko prieš mane neturi. Jei būtų turėję, tai kodėl Meistras Splyntras nesiuntė Turkijos policijai jokios informacijos, kurią ji būtų galėjusi panaudoti prieš

mane? – paklausė jis. – Tačiau, mėgindami sugauti mane, jie tesugebėjo panaudoti tą smulkų niekšelį Ortaçą." Tada Çağatay'us pareiškė, kad jis įsilaužė į Mularskio duomenų bazę ir išgavo iš jos visą informaciją, kurią FTB surinko apie visus Tamsiosios rinkos narius, taip pat ir medžiagą apie save.

Sėdėdamas kalėjime, Çağatay'us, be abejonės, negalėjo dokumentais patvirtinti savo teiginių. Jis sakė nuo pat pradžių žinojęs, kad Splyntras buvo FTB agentas (nors Çağatay'us JiLsi kvietimu įstojo į Tamsiąją rinką 2006 m. vasarį, kai Meistras Splyntras buvo jau pakankamai gerai įsitvirtinęs forume) ir kad jis laikėsi strategijos „laikyti draugus arti savęs, o priešus dar arčiau" – iš čia ir jo noras dirbti su administratoriumi Splyntru.

Tai buvo tinkama tema pokalbiui užbaigti. Tamsiosios rinkos istorija iš esmės susijusi su dviem vyriškiais – Çağatay'umi Evyapanu ir Keithu Mularskiu, kurie abu turėjo įspūdingas komandas ir bendraminčių. Cha0 nebuvo eilinis nusikaltėlis. Nors svarbiausias šio sumanymo tikslas buvo užsidirbti pinigų, atrodo, jog Çağatay'ui kova su teisėsauga turėjo gilesnę prasmę, tarsi jis būtų siekęs pademonstruoti savo pranašumą ir, kaip galima numanyti, bergždžias teisėsaugos pastangas kontroliuoti kibernetinę erdvę. Čia slypi originalus kompiuterių ir kibernetikos fanatikų kultūros anarchizmas – elgesio modeliai ir moraliniai principai keičiasi, pereinant iš realaus pasaulio į virtualų. Žaidimo taisyklės čia naujos ir kitokios.

FTB agentas šį sykį nugalėjo, bet tai buvo nedidelė pergalė ir jokiu būdu ne galutinė. Prabėgus trejiems metams po Tamsiosios rinkos uždarymo, šios neeilinės kriminalinės avantiūros atgarsiai aidi įvairiuose pasaulio kalėjimuose ir teismuose. Ir, be abejo, daug Tamsiosios rinkos dalyvių vis dar išdidžiai staiposi internetinėje erdvėje.

Internetas – tai transcendentinis išradimas, kuris įsismelkė į visas mūsų gyvenimo sritis ir į kiekvieno iš mūsų namus. Tačiau saugokitės – galbūt kokioje nors virtualioje spintelėje slepiasi Lordas Cyrikas.

EPILOGAS

Iš pirmo žvilgsnio atrodo, kad Tamsiosios rinkos žlugimas sudavė rimtą smūgį internetiniams nusikaltimams. Bet taip neatsitiko. Šiaip ar taip, jis laikinai sutrikdė kai kurių svarbesnių kardingo tinklų darbą, tarp jų ir Cha0 veiklą Turkijoje, Maksiko Ukrainoje ir Freddybb Anglijoje. Bet svarbiausias dalykas, kurį kiti rimti kibernetiniai nusikaltėliai sužinojo iš visos šios aferos, buvo visai paprastas: dalyvavimas tokiuose kardingo forumuose kaip „Shadowcrew" ir „DarkMarket", o ypač anglakalbių interneto svetainėse su daugybe narių, dabar įgavo nepriimtiną rizikos laipsnį.

Jau būta tam tikrų įrodymų, kad narių, kurių pagrindinis tikslas buvo uždirbti pinigų, o ne sustiprinti savo autoritetą, „DarkMarket" forume buvo daug mažiau nei „Shadowcrew". Skaičius pranešimų, kuriuos skelbė tokie žmonės kaip Freddybb, „DarkMarket" svetainėje buvo gerokai mažesnis nei „Shadowcrew". Svetainėje „Shadowcrew" jis paskelbė penkiasdešimt viešų pranešimų ir du šimtus privačių. „DarkMarket" svetainėje šių pranešimų skaičius atitinkamai buvo penkiolika ir dvylika. JAV slaptoji tarnyba, išardžiusi „Shadowcrew", aiškiai pademonstravo šių interneto svetainių pažeidžiamumą, o Freddybb išmoko pamoką: būk mažiau matomas.

Nors ir grėsė pavojus sužlugti, vis dėlto kardingo forumai atliko savo vaidmenį. Naudodamiesi šiomis interneto svetainėmis, per beveik dešimtį veiklos metų nusikaltėliai sukūrė pasaulinius tinklus žmonių, kuriais galėjo pasitikėti. Jie rado rinką, kurioje galėjo pirkti ar parduoti nelegaliai įgytus duomenis ir dokumentus.

Tačiau Keitho Mularskio, kaip Meistro Splyntro, demaskavimas ir fakto, kad „DarkMarket“ iš dalies buvo operacija su teisėsaugos paspęstomis pinklėmis, atskleidimas neabejotinai pagreitino kardingo forumų žlugimą. Tai sugriovė FTB ir jos partnerių Vakarų Europoje ilgalaikę strategiją. Pagal planą Meistras Splyntras turėjo vėl pasirodyti kaip doruolis karderis, sužlugdęs FTB pastangas juos pagauti ir dėl to nusipelnęs dar didesnio kardingo brolijos pasitikėjimo.

O dabar, reaguodami į Tamsiosios rinkos aferą, programišiai, įsilaužėliai ir kibernetiniai nusikaltėliai dar giliau pasislėpė skaitmeniniame pogrindyje. Šiame versle taip pat didėja specializacija. Programišiai ir kenkėjiškų programų kūrėjai kuria įmantrias programas, skirtas panaudoti konkrečiose sistemose arba tam tikros rūšies informacijai išgauti. Tada parduoda jas grupėms, kurios iš tiesų vadovauja skverbimuisi į finansines institucijas ir jų klientų duomenų bazes. Galėdamos prieiti prie pinigų, jos susisiekia su „mulų varovu“ – asmeniu ar grupe, kurie samdo „pinigų mulus“ iš viso pasaulio. Interneto svetainėse galima rasti nesuskaičiuojamą daugybę reklaminių skelbimų, siūlančių žmonėms darbą, naudojantis savo namuose esančiu kompiuteriu. Daug tokių skelbimų įdeda „mulų varovai“. „Varovai“ prašo potencialių „mulų“ perduoti savo banko sąskaitas „varovų“ dispozicijai, o mainais siūlo tam tikrą procentą nuo per jas pervedamų pinigų srautų.

Dėl kriminalinės veiklos išskaidymo į atskirus subjektus teisėsaugai sunkiau nustatyti, kas iš tiesų vyksta ir kas su kuo bendradarbiauja. Milžiniškų galimybių kibernetiniams nusikaltėliams taip pat suteikia ir mobiliųjų prietaisų ir reikmenų plitimas.

Kadangi sparčiai daugėja interneto vartotojų, atsiranda kita svarbi problema. Vakarų Europos policija pastebėjo, kad greitai auga kinų programišių bendruomenė. Dar neseniai „419“, arba vadinamojo „sukčiavimo su išankstiniu apmokėjimu“, monopolį turė-

jo Vakarų Afrikos, ypač Nigerijos, kriminalinės grupės – įspūdingi kūrėjai tų įmantrių elektroninių laiškų, kuriuose gavėjas maldaujamas padėti skubiai pervesti milijonus mirusio diktatoriaus dolerių.

„419“, pavadintas pagal atitinkamą Nigerijos baudžiamojo kodekso paragrafą, yra labai senas triukas – juo paremtas karalienės Elžbietos laikų pjesių autoriaus Beno Jonsono komedijos *Alchemikas* siužetas. Iš esmės sukčius įkalba savo auką pervesti šiek tiek pinigų, žadėdamas, kad vėliau auka gaus daug didesnę sumą. Paskui jis arba išprašo iš aukos dar daugiau pinigų, arba paprasčiausiai dingsta su pirmąja įmoka. Elžbietos laikais tai buvo nors ir įmanomas, bet daug pastangų reikalaujantis užsiėmimas. Dėl interneto galimybių jis pasidarė labai pelningas, nes, naudodamas brukamus elektroninius laiškus, nusikaltėlis gali pasiekti dešimčių milijonų auditoriją. Šansai rasti mulkį smarkiai padidėja.

„419“ suktybė būna įvairių formų ir mastų. Kartais ji ateina kaip kreipimasis į turtingus vakariečius padėti skurdo nualintam Afrikos vaikui. Amerikiečiai dažnai gauna laiškų, faksogramų ir elektroninių žinučių, kuriuose prašoma lėšų tam tikriems tikslams, pavyzdžiui, naujai bažnyčiai statyti arba parapijai paremti. Šiais atvejais aukų motyvacija būna pagrįsta gerais ketinimais ir labdara. Kitas pelningas „419“ sukčių grobis yra ištroškusieji meilės, ypač vidutinio amžiaus našlės ir išsiskyrusios moterys, kurios užmezga virtualius santykius su flirto partneriais – vaikinais iš Vakarų Afrikos, o šie palengva išsiurbia jų santaupas, žadėdami seksualinius santykius, nors jų niekada nebūna.

„419“ dabar yra siunčiami iš Kinijos tiek kinų, tiek anglų kalbomis. Tai papildo kitą kinų programišių specializaciją – vagystes iš vadinamųjų MMORPG (gremėzdiško pavadinimo „Labai didelio žaidėjų skaičiaus internetiniai vaidybiniai žaidimai“ gremėzdiška santrumpa), pavyzdžiui, „Karo meno pasaulio“ (*World of Warcraft*) arba vadinamųjų realaus gyvenimo žaidimų, kaip antai „Antrasis

gyvenimas" (*Second Life*) arba „Habbo viešbutis" (*Habbo Hotel*). Visuose šiuose žaidimuose egzistuoja skaitmeninė valiuta, kuri gali būti iškeista į tikrus pinigus. Pastaruosius savo ruožtu pagal vertę galima investuoti į virtualias prekes ir paslaugas, kurias žaidėjai gali nusipirkti kaip priedą prie to malonumo, kurį patiria žaisdami žaidimus. Kinų programišiai (tačiau ne vien jie) išmoko „pavogti" šiuos skaitmeninius vienetus arba pinigus ir konvertuoti juos į tikrus realiame pasaulyje naudojamus grynuosius. Šiuo metu milžiniškas Kinijos kompiuterių naudojimo potencialas išlieka didele dalimi nepanaudotas, nors daugelyje su kompiuterių saugumu susijusių civilinių ir karinių sričių jis jau laikomas antruoju pagal pasaulinę hierarchiją po Jungtinių Amerikos Valstijų. Kai Kinija pradės realizuoti šį potencialą, interneto prigimtis pasikeis.

Norėdami įveikti šias didėjančias grėsmes, vyriausybės ir pramoninkai šiandien investuoja šimtus milijardų dolerių į kibernetinį saugumą – ar tai būtų teisėsauga, ar intelektinių autorinių teisių apsauga, ar karinė sritis. Beveik visos šios lėšos yra investuojamos į technologijas, vadovaujantis idėja, jog reikia apsaugoti internetą nuo visų blogų, kenkėjiškų programų ir virusų, klaidžiojančių po kibernetinę erdvę ir ieškančių neapsaugotų kompiuterinių tinklų, kuriuos galėtų atakuoti, ir to pakaks.

Deja, iš esmės visai neinvestuojama siekiant nustatyti, kas įsilaužia į kompiuterius ir kokiais tikslais. Niekas neatskiria „programišių iš „WikiLeaks" nuo programišių iš Amerikos ar Kinijos karinės pramonės, o kriminalinių sindikatų – nuo paprasčiausių smalsuolių.

Tačiau programišiai yra labai reta ir ypatinga žmonių rūšis. Apskritai jų psichologinės ir socialinės charakteristikos svyruoja nuo būdingų tradiciniams kriminaliniams nusikaltėliams iki tų, kurios yra esminės, norint atverti duris kriminalinio verslo galimybėms internete, kai nėra per daug domimasi pinigais – kitaip tariant,

būdingos kompiuterių fanatikams. Jų sugebėjimų ir motyvacijos įsitraukti į specifinius užsiėmimus, ar jie būtų kriminaliniai, ar kokie kitokie, suvokimas duotų milžinišką naudą saugumo pramonei, kuri yra pernelyg priklausoma nuo techninių sprendimų. Tais retais atvejais, kai teisėsauga ar privatus sektorius atseka programišius, o tada jie patraukiami baudžiamojon atsakomybėn ir nuteisiami, labai mažai domimasi santykiais su pačiais pažeidėjais. Europos ir Jungtinių Valstijų kriminalinės teisėsaugos tik siekia juos nuteisti, paskirti sunkias laisvės atėmimo bausmes, o paskui suvaržyti jų priėjimą prie kompiuterių.

Žinant jų specifines psichologines ir sociologines charakteristikas, tai didelė klaida. Visų pirma reikia atsižvelgti į jų amžių: dauguma programišių labai jauni įsitraukia į veiklą, kurią geriausiai būtų galima apibūdinti kaip teisiniu požiūriu dviprasmišką. Panašiai kaip Detlefas Hartmannas, jie gali susivilioti nelegaliu darbu internete anksčiau, nei tinkamai išsivysto jų moralės kompasas, ir anksčiau, nei visiškai supranta to, ką daro, prasmę.

Realiame gyvenime jie dažnai būna psichologiškai pažeidžiami, o tai reiškia, kad, atstūmus juos ir palikus tarp tikrų nusikaltėlių, galima sulaukti labai neigiamų rezultatų, kaip tai atsitiko Maksui Vizijai. Nors jo ego neprognozuojamas, visi pareigūnai sutinka, kad Vizija turi planetos dydžio smegenis ir kaip niekas kitas išmano kompiuterių saugumo klausimus. Atrodo, kad pasaulyje, kur trūksta kompiuterių saugumo specialistų ir vis daugėja grėsmių, nėra išmintinga įkalinti fenomenalų turtą. Tai nereiškia, kad programišiai, kurie įsitraukia į nusikalstamą veiklą, turėtų išvengti bausmės, bet reikiamybė juos reabilituoti yra ne tik moralinė būtinybė valstybei, bet ir turi didelę potencialią praktinę reikšmę.

Buvęs programišius Raoulis Chiesa vadovauja mažam akademiniam centrui pavadinimu „Programišių profiliavimo skyrius“, įsikūrusiam Turine ir finansuojamam Jungtinių Tautų. Jo tyrimai

paremti asmeninėmis žiniomis apie programišių bendruomenę ir programišių atsakymais į išsamias anketas, kurias jis jiems išsiuntinėja. Jau pirmieji jo darbo rezultatai siūlo svarbius būdus programišių prigimčiai perprasti.

Labiausiai stebina lyčių disbalansas, būdingas ne tik nelegalioms internetinės veiklos sritims, bet ir interneto, kaip visumos, organizacijai ir veikimui. Tai tema, apie kurią šios knygos puslapiuose tik užsimenama, bet ji nusipelno išsamios studijos. Nors viso pasaulio politikoje ir ekonomikoje vis dar dominuoja vyrai, šis dominavimas yra ypač ryškus, kai kalbama apie naujas technologijas. Be abejo, esama labai veiklių moterų, besidominčių naujomis technologijomis ir naująja žiniasklaida, tačiau statistiškai jos sudaro labai menką procentą: remiantis Chiesos duomenimis, tik 5 procentus. Programišiai yra beveik vien vyrai.

Kitas Chiesos studijos atradimas yra tas, kad vidutinis programišius yra arba gabus, arba labai gabus. Dar daugiau, jis pastebėjo, kad labai dažnai, beveik šimtu procentų, programišiai yra nepaprastai gabūs tiksliesiems mokslams – fizikai, matematikai ir chemijai. Tai dera su palyginti prastais sugebėjimais humanitarinių mokslų srityje.

Galiausiai svarbus klausimas yra programišių santykiai. Daugumai jų, nors ne visiems, daug lengviau užmegzti santykius nuasmenintoje interneto aplinkoje nei realiame gyvenime. Įdomu kodėl.

Paprastai programišiai pradeda reikštis paauglystėje, būtent tada, kai dauguma susiduria su sunkumais užmegzti santykius, ypač su priešinga lytimi. Taigi, bent jau iš dalies, jų sunkumai šioje srityje yra visiškai natūralūs. Tačiau Chiesa taip pat nustatė, kad neįprastai daug programišių anketose rašė apie bendravimo problemas šeimoje, o labiausiai – su savo tėvais.

Skaitydamas Chiesos studiją ir daug laiko praleidęs kalbėdamasis su įvairių rūšių programišiais, aš prisiminiau Kembridžo uni-

versiteto vystymosi psichopatologijos profesoriaus Simono Barono-Coheno darbus. Jo novatoriškas darbas apie autizmą leido geriau suprasti vyriško ir moteriško elgesio modelių spektrą. Iš esmės tipiški vyriškosios giminės atstovai geriau geba sistematizuoti išorinį pasaulį, o tipiškos moteriškosios giminės atstovės turi daugiau sugebėjimų įsijausti. Tuo nenorima pasakyti, kad visos moterys prastai susigaudo žemėlapiuose, o visi vyrai beviltiškai nemoka išklausyti, o tik tai, kad kiekviena lytis pasižymi aiškiai išreikšta tendencija: vyrai – sistematizavimu, o moterys – įsijautimu.

Tolesni Barono-Coheno tyrimai leido jam atskleisti sąryšį tarp aukščiausio laipsnio vyriško proto, kuris tam tikromis aplinkybės galėtų būti apibūdintas kaip „autistinis", ir aukšto hormono testosterono lygio, kuris gali paveikti gimdoje esantį vaisių. Jo tezė yra ginčytina, bet, kalbant apie programišius ir jų elgesio modelius, daugeliu atžvilgių įtikinama ir neabejotinai vertinga. Be abejo, ne visi programišiai yra autistai; iš tiesų tokių yra labai nedaug (nors keletui iš garsių programišių, pavyzdžiui, Gary'iui McKinnonui, paieškomam Jungtinėse Valstijose dėl įsilaužimo į Pentagoną, buvo diagnozuotas Aspergerio sindromas). Bet tokių yra ir jie atitinka daugelį klinikinių stebėjimų, kuriuos aprašė profesorius Baronas-Cohenas, tyrinėdamas asmenis, atsidūrusius gana tolimame „vyriškojo" spektro gale.

Toliau tyrinėjant, galima padaryti išvadą, kad ateityje bus įmanoma nustatyti programišių asmenybės tipus tarp vaikų, dar tebesimokančių mokykloje. Tokiu atveju bendraamžiai ir auklėtojai galėtų skatinti jų gabumų vystymą, tuo pat metu suteikdami jiems moralinę paramą, kad jų gabumai būtų nukreipti teigiama linkme. Žodis „programišius" turi neigiamą atspalvį. Tačiau sugebėjimas įsilaužti faktiškai yra turtas tiek asmeniniu, tiek socialiniu požiūriu. Kompiuteriai ir jų tinklai niekada nebus saugūs, jei jų neapsaugos pažangūs programišiai. Kai kurie iš tokių individų jau dirba šioje

srityje. Kiek žinau iš savo patirties, 90 procentų programišių, dalyvaujančių kriminalinėje veikloje, yra išreiškę didelį norą dirbti legalioje saugumo pramonėje – ir, be abejo, net ir tiems, kurie yra teisti, turėtų būti suteikta tokia galimybė.

Adewale'as Taiwo, dar žinomas kaip Freddybb

2009 m. sausio 1 d. Halo miesto Karališkasis teismas nuteisė Adewale'ą Taiwo ketverių metų laisvės atėmimo bausme už bendrininkavimą sukčiaujant nuo 2004 m. birželio iki 2008 m. vasario. Praėjusį lapkritį jis jau buvo prisipažinęs esąs kaltas, apgaulės būdu paėmęs iš įvairių banko sąskaitų visame pasaulyje beveik 600 000 svarų. Teisėjas rekomendavo, kad atlikęs bausmę jis būtų deportuotas į Nigeriją.

Už gerą elgesį sutrumpinus bausmės laiką, Taiwo turėjo būti paleistas 2010 m. rugpjūčio 29 d. Dviem savaitėmis anksčiau jis pasirodė kitoje Hamberio upės žiočių pusėje esančio Grimsbio miesto teisme. Byla buvo nagrinėjama, remiantis Britanijos įstatymu dėl nusikalstamu būdu įgytų pajamų, vienu iš nedaugelio protingų Tony Blairo kriminalinės teisėtvarkos sistemos patobulinimų, kuris valstybei suteikė galimybę atgauti lėšas iš nusikaltėlių. Rimta byla baigėsi absurdiškai. Prokuroras kažkur nukišo pagrindinį dokumentų aplanką, ir tai sukėlė netikėtą barzdoto teisėjo Grahamo Robinsono reakciją: iš pradžių puikus jo humoro jausmas greitai virto pykčiu. Jis paskelbė neketinąs atidėti teismo posėdžio, taigi abi šalys turėtų kuo greičiau pasiekti susitarimą. Tai labai sustiprino Adewale'o pozicijas. Teisėjas galiausiai paskelbė, kad teisiamasis turės sumokėti šiek tiek daugiau nei 53 000 svarų, nors pradinis žalos įvertinimas sudarė 353 067 svarų. Taiwo pareiškė, kad nemokės šių pinigų, o tai reiškė, kad jam teks atsėdėti dar vienus metus kalėjime.

Faktiškai 2011 m. balandžio 7 d. jis buvo deportuotas į Nigeriją. Taiwo, vienam iš sumaniausių veikėjų, savo dalyvavimu pagerbusių kardingo forumus, beveik pavyko gyventi dvigubą talentingo chemijos inžinieriaus ir kibernetinio nusikaltėlio gyvenimą.

Detektyvas seržantas Chrisas Dawsonas

Detektyvas seržantas Chrisas Dawsonas su išskirtiniu uolumu dirbo prie Freddybb bylos, skirdamas jai daug asmeninio laiko, kad užtikrintų, jog skaičių, datų ir technologinių detalių kratinys, pasiekęs teismą, būtų suprantamas bet kuriam neprofesionalui. Per Taiwo nusikalstamu būdu gautų pajamų bylos nagrinėjimo posėdžio pertraukas, skirtas konsultacijoms, Dawsonui pasirodė, jog jis išgirdo Taiwo sakant: „Po velnių, aš nemokėsiu." Kai teisėjas išėjo iš teismo salės, detektyvas išlėkė laukan įsiutęs dėl Anglijos teisinės sistemos nekompetentingumo.

Jis tebedirba vyresniuoju žmogžudysčių skyriaus pareigūnu Halo mieste.

Dimitrijus Golubovas

Programišius Dimitrijus Golubovas po arešto Odesoje praleido kalėjime penkis su puse mėnesio: per tą laiką jį tardė Amerikos teisėsaugos pareigūnai, tarp jų JAV pašto inspekcijos tarnybos pareigūnas Gregas Crabbas. Tačiau įsikišus dviem Ukrainos parlamento nariams, jis buvo paleistas ir galiausiai 2009 m. Kijevo teisme reabilituotas dėl bet kokių įstatymų pažeidimų.

Beveik 190 cm ūgio, įdėmaus charizmatiško mėlynų akių žvilgsnio Golubovas neigia bet kokius santykius su Skriptu, nors jo

įvykių versijoje yra nesuderinamumų, o Amerikos teisėsaugos turimi skaitmeniniai įrodymai patvirtina visai kitokią istoriją (tarp jų yra Romano Vegos kompiuteryje rasti duomenys apie tai, jog Skriptas yra Golubovas).

Skriptas išgaravo, kai Golubovas buvo paleistas iš kardomojo įkalinimo, bet pats Golubovas grįžęs vėl įsitraukė į veiklą, susijusią su socialiniais pokyčiais ir iniciatyvomis, ir įsteigė Ukrainos interneto partiją. Tebegyvenantis Odesoje Golubovas sukūrė politinę programą, kurios tikslas – kovoti su korupcija, pornografija ir narkotikų verslu internete. Jis įsitikinęs, kad per dešimtmetį bus išrinktas Ukrainos ministru pirmininku arba prezidentu, ir nors šiuo metu tai atrodo kaip rizikingiausios lažybos, į jo veržlumą ir ambicijas vertėtų žiūrėti rimtai. Interneto partija vietinių tarybų rinkimuose Odesoje iškėlė dešimtis savo kandidatų, ir nors iki šiol laimėjo tik vieną vietą, nėra jokių abejonių, kad judėjimas plinta visoje šalyje.

Vis dėlto keista, kad nepaisydamas ryžtingo savo organizacijos moralinio pasipriešinimo kai kuriems nusikalstamiems veiksmams, pavyzdžiui, pornografijos platinimui, Golubovas pradėjo kampaniją, kurios tikslas – pasiekti, kad įžymus karderis Maksikas būtų atleistas nuo trisdešimties metų laisvės atėmimo bausmės Turkijoje.

Romanas Vega

Romanas Vega buvo suimtas ir įkalintas Nikosijoje 2003 m. vasarį. Nuo tada, kai Jungtinių Valstijų prašymu 2004 m. birželį buvo perkeltas į Kaliforniją, jis laikomas kalėjime, bet niekada nebuvo teisiamas. Tuo metu, kai buvo rašoma ši knyga, jis kalėjo Municipaliniame sulaikymo centre Brukline, niūriame pastate netoli Govanuso įlankos. Per visą tą laiką Vega nesulaukė jokių lankytojų, išskyrus savo juridinius atstovus.

2007 m. rugpjūtį Kalifornijos šiaurinėje apygardoje turėjo įvykti posėdis, teisėjaujant Charlesui R. Breyeriui. Kaltintojas ir gynėjas buvo pasiruošę posėdžio pabaigoje pasirašyti taikų susitarimą, pagal kurį Vega būtų buvęs paleistas, atsėdėjęs keturiasdešimt šešis mėnesius jam paskirtos bausmės. Popietę prieš numatomą jo paleidimą kaltintojas iš Niujorko rytinės apygardos pateikė visą sąrašą naujų kaltinimų, reikalaudamas perkelti Vegą į Brukliną. Kaltinimai iš esmės buvo tokie pat kaip ir pateiktieji Kalifornijoje. Tačiau, norėdamas išvengti dvigubo apkaltinimo, kaltinamojo advokatas iš Niujorko paprašė taikyti kitą statutą kaltinimams suformuluoti.

Iš teismo posėdžio protokolo aiškiai matyti, jog teisėjas Breyeris, Aukščiausiojo teismo nario Stepheno Breyerio brolis, buvo sutrikęs ir pasipiktinęs Niujorko rytinės apygardos teismo taktika. Naujas kaltinimas buvo paremtas informacija, kurią pateikė JAV slaptosios tarnybos agentai.

Kai Vega atvyko į Brukliną, Slaptoji tarnyba pasiūlė jam sandėrį: jei jis sutiktų liudyti prieš Dimitrijų Golubovą ir kitus Ukrainos organizacijos narius (ne programišius, o aukštesnes politines figūras), tada jie atsiimtų kaltinimus. Bet jei jis atsisakytų, jie pareikštų jam dar daugiau kaltinimų, remdamiesi įvairiose valstijose saugomais dokumentais. Jie tai tęstų, kol jis sutiktų bendradarbiauti.

Nepriklausomai nuo to, ką Vega padarė ar ko nepadarė, jis jau atsėdėjo kalėjime tris kartus ilgiau nei kiti, nuteisti už savo veiklą „Shadowcrew" komandoje. Virš jo galvos dar kabo dvi neišspręstos bylos ir grėsmė, kad jų gali būti ir daugiau. Keletą metų Vegą vargina stiprus dantų ėduonis, jis nuolatos kenčia skausmą ir dažnai negali normaliai pavalgyti. Kalėjimų departamento ir JAV maršalų tarnybos* sprendimu buvo atsisakyta jam suteikti medicininę pagalbą.

Neatrodo, kad artimiausioje ateityje Vega bus paleistas.

* Jungtinių Valstijų maršalų tarnyba (angl. *The United States Marshals Service*) yra Jungtinių Amerikos Valstijų federalinė įstatymų priežiūros tarnyba prie Jungtinių Valstijų teisingumo departamento.

Maksimas Kovalčiukas, dar žinomas kaip Blade*

Kovalčiukas buvo suimtas 2003 m. gegužę Tailande ir išduotas Jungtinėms Valstijoms, kur atsėdėjo kalėjime ketverius metus. FTB pritarė po derybų pasirašytam taikiam susitarimui ir 2007 m. pabaigoje jis buvo paleistas, o tada anonimiškai grįžo į Ukrainą. FTB sprendimas jį paleisti yra akivaizdi priešingybė Slaptosios tarnybos sulaikymo taktikai, kuri taikoma Romanui Vegai.

Ręnukanthas Subramaniamas, dar žinomas kaip JiLsi

2010 m. vasario 26 d. Subramaniamas prisipažino dėl vieno kaltinimo sukčiavimu su kreditinėmis kortelėmis ir dėl keturių kaltinimų sukčiavimu įkeičiant nekilnojamąjį turtą, už kuriuos Blakfrajerio karūnos teismas nuteisė jį ketverių metų laisvės atėmimo bausme. Visą knygos rašymo laiką jis buvo įkalintas vakarų Londono „Wormwood Scrubs“ kalėjime, kur teko kalėti ir kompozitoriui serui Michaeliui Tippettui bei roko grupės „Rolling Stones“ gitaristui Keithui Richardsui.

Subramaniamas tikisi, kad už gerą elgesį bus paleistas anksčiau laiko – 2012 m. liepos pabaigoje. Didžioji jo bylos dalis susijusi ne su Tamsiąja rinka, o su sukčiavimais įkeičiant nekilnojamąjį turtą. Į kaltinimą yra įtraukti penki tokie atvejai (tiesa, tris iš šių pareiškimų atmetė finansinės institucijos). Nors sukčiavimai įkeičiant nekilnojamąjį turtą yra atskiros rūšies nusikaltimai, kaltinime užsimenama apie ryšį tarp Subramaniamo uždarbio iš Tamsiosios rinkos ir jo galimybės sumokėti paskolų įmokas. Faktiškai Subramaniamas teigė nesąs atsakingas už paskolų įmokas, nes prašė pa-

* *Blade* – ašmenys. (Angl.)

skolų savo draugų vardu, kadangi šie patys negalėjo to padaryti. Be to, Subramaniamas laukia savo bylos dėl nusikalstamu būdu įgytų pajamų posėdžio išvadų, kad sužinotų, ar jam bus priteistas turto konfiskavimas. Pagal nusikaltimų prevencijos orderiu numatytas sąlygas, paleistas iš kalėjimo jis penkerius metus negalės be priežiūros naudotis kompiuteriu.

Detlefas Hartmanas, dar žinomas kaip Matrica (Matrix001)

2007 m. spalio 9 d. Štutgarto apygardos teismas nutarė, kad Hartmannas turi būti teisiamas dėl trylikos sukčiavimo su kreditinėmis kortelėmis atvejų. Tačiau tas pats teismas paskelbė, kad siūlymas patraukti jį baudžiamojon atsakomybėn dėl nusikalstamo susivienijimo suformavimo atmestas. Kadangi rimtesnis kaltinimas buvo atmestas, Hartmannas buvo paleistas iš Štamheimo kalėjimo, kur praleido keturis mėnesius. Pagrindinis sprendimas, užkirtęs kelią jo kaltinimui sąmokslu, susijęs su tuo, kaip teismas interpretavo Vokietijos pagrindinį įstatymą – konstituciją, kurioje teigiama, kad susivienijimo narys turi priklausyti „jungtinei grupei“, kurioje yra numatytas „individo pavaldumas kolektyvo valiai“. Teisėjas įrodinėjo, kad nestabilus interneto ir Tamsiosios rinkos struktūrų pobūdis neatitinka šių kriterijų, – sprendimas, kuris, be abejo, turi svarbią reikšmę įstatymų, susijusių su internetiniais nusikaltimais Vokietijoje, kūrimui.

2008 m. liepą Hartmannui buvo paskirta lygtinė dvidešimt vieno mėnesio bausmė už sukčiavimą. Nuo tada jis vėl užsiėmė grafinio dizaino studijomis ir visiškai nutraukė bet kokius ryšius su pogrindžiu.

Raudonoji Brigada (RedBrigade)

Jis iš esmės metė nesąžiningus darbelius ir šiuo metu yra Europoje.

Maksas Vizija (Max Vision), dar žinomas kaip Maxas Butleris ir kaip Ledo Žmogus (Iceman)

2010 m. vasario 12 d. Pitsburgo teismas nuteisė Maksą Viziją trylikos metų laisvės atėmimo bausme. Tai ilgiausias įkalinimo terminas, Amerikos teismo kada nors paskelbtas dėl kompiuterinių įsilaužimų. Kaltinančioji šalis apskaičiavo, kad dėl Makso Vizijos įsilaužimų kreditinių kortelių nuostoliai siekė daugiau nei 85 milijonus dolerių. Dabar jis kalinamas negriežto režimo Lompoko federalinėje pataisos įstaigoje, esančioje Lompoko mieste pietinėje Kalifornijoje. Ten jam neleidžiama naudotis jokiais kompiuteriais.

Vizijos įsilaužimo galimybės neprilygstamos – jis neabejotinai yra vienas iš sumaniausių vyrukų, atliekančių bausmę Jungtinėse Valstijose. 2010 m. rudenį uždaroje konferencijoje aš kalbėjausi apie jo bylą su vienu iš aukštesniųjų pareigūnų iš Krašto apsaugos departamento, užsiimančio kibernetinių grėsmių klausimais. Jis sutiko su manimi, kad kompiuterių specialisto, turinčio tokių gabumų kaip Vizija, nykimą kalėjime galima laikyti netinkamu JAV žmogiškųjų išteklių panaudojimu, tačiau pareiškė, jog Vizijos ego – beveik toks pat didžiulis kaip ir jo intelektas – taip pat suvaidino svarbų vaidmenį šioje aferoje.

Nicholas Joehle'as, dar žinomas kaip Dronas

Joehle'as buvo paleistas iš kalėjimo, atlikęs bausmę už sukčiavimą kreditinėmis kortelėmis ir nelegalią kreditinių kortelių duomenų nuskaitymo įrenginių gamybą.

Hakimas B, dar žinomas kaip Lordas Kaisersose'as

Lordas Kaisersose'as gyvena Marselyje ir vis dar laukia teismo, bet yra paleistas už užstatą. Prancūzija yra dar viena šalis, kur teisingumo ratus vertėtų šiek tiek sutepti, kad jie greičiau suktųsi.

Cha0

Cha0 arba turi verslą Slovėnijoje, arba sėdi kalėjime. Viskas priklauso nuo to, ar tikrasis Cha0 yra Şahinas, ar Çağatay'us Evyapanas. Pastarajam yra paskirtas kardomasis kalinimas viename iš Turkijos griežto režimo kalėjimų Tekirdahe. Jo teismo procesas turi prasidėti šiais metais, bet kaltintojas atmetė rimtesnius kaltinimus, susijusius su organizuotu nusikalstamumu.

Mertas Ortaças, dar žinomas kaip SLayraCkEr

Mertui buvo paskirtas kardomasis kalinimas Stambulo kalėjime dėl kaltinimų, susijusių su banko „Akbank" byla, bet 2010 m. kovą dėl techninių aspektų jis buvo paleistas. Jis vėl buvo suimtas 2010 m. lapkritį ir rašant knygą tebebuvo sulaikytas kardomajam kalinimui. Mertas, nors aikštingas ir nenuspėjamas, buvo vienas iš talentingiausių Tamsiosios rinkos dalyvių.

Keithas Mularskis ir Bilalas Şenas

Jie abu ir toliau patruliuoja nedorėlių pilnose kibernetinėse erdvėse.

Lordas Cyrikas

Kas jis? Medžioklė tęsiasi...

PASTABOS APIE DUOMENŲ ŠALTINIUS

Diduma šioje knygoje pateiktos informacijos yra iš 2009–2011 m. mano paimtų interviu, kurių bendra trukmė sudaro maždaug 200 valandų. Keletą valandų interviu taip pat sutiko paimti Leonida Krushelnycky*.

Be to, aš rėmiausi dviem pagrindiniais dokumentiniais šaltiniais. Pirmasis yra teismų protokolai iš daugelio teismų procesų, susijusių su interneto svetainėmis „CarderPlanet", „Shadowcrew" ir „DarkMarket". Antrasis yra pačių svetainių archyvai, ypač dviejų pirmųjų svetainių, – jie lengvai prieinami internete. Deja, sunkiau prieiti prie „DarkMarket" archyvų. Žinau tik apie vieną archyvą, priklausantį FTB, tačiau biuras dėl operatyvinių priežasčių negali leisti juo naudotis.

Literatūros apie kibernetinius nusikaltimus, kibernetinį pramoninį šnipinėjimą ir kibernetinius karus yra gana daug ir nemažai jos galima rasti internete. Dėl informacijos visapusiškumo norėčiau paminėti Kevino Poulseno ir jo komandos darbą, – jo tinklaraštis (angl. *blog*) *Threat Level* („Grėsmės lygis") yra ne tik gerai parašytas, bet ir medžiaga gerai išnagrinėta. Aš rekomenduočiau dvi knygas, kuriose konkrečiai aptariami kibernetiniai nusikaltimai. Tai Kevino Poulseno *Svarbiausias elementas* (*Kingpin*) ir Josepho Menno *Lemtinga sistemos klaida* (*Fatal System Error*). Tie, kurie nori pla-

* BBC žurnalistė.

čiau susipažinti su kai kuriais iššūkiais, susijusiais su internetinėmis technologijomis, turėtų pradėti nuo Jonathano Zittraino *Interneto ateitis: Ir kaip ją sustabdyti* (*The Future of the Internet: And How to Stop It*).

Tarp kitų vertingų tinklaraščių paminėtini Briano Krebso *Krebsonsecurity*, Bruce'o Schneierio informacinis biuletenis *Cryptogram*, suomių kompiuterinio saugumo kompanijos „F-Secure" tinklaraštis ir galiausiai Dancho Danchevo ir Ryano Naraine tinklaraštis *Zero Day* („Nulinė diena") interneto svetainėje „Z Net".

PADĖKOS

Šios knygos rašymas pateikė daug iššūkių, kurių aš niekada nebūčiau įveikęs, jei nebūčiau sulaukęs daugelio draugų ir kolegų iš viso pasaulio kilniaširdiškos paramos.

Britanijoje svarbiausią vaidmenį suvaidino du žmonės. Leonida Krushelnycky įrodė esanti nenuilstanti tyrėja, ji dažnai atskleisdavo svarbią medžiagą, kai aš jau seniai būdavau praradęs bet kokią viltį ją surasti. Be jos pastangų knyga būtų buvusi daug skurdesnė. Vesna Vucenovic užtikrino, kad šio projekto administravimas būtų kuo lengvesnis.

Keliaudamas turėjau laimės susitikti su dviem žurnalistais, kurių kantrybė ir malonus elgesys atitiko jų aukščiausio lygio profesionalumą ir gebėjimus. Kai'us Laufenas padėjo man perprasti sudėtingą Vokietijos teisingumo sistemą. Bet jo pagalba buvo dar vertingesnė dėl pažinčių, kurias jis man padėjo užmegzti, ir svetingumo, kurį jis man suteikė. Lygiai taip aš būčiau visiškai pasimetęs Stambule ir Turkijoje, jei ne Sebnem Arsu. Atkakli, visuomet mandagi ir sugebanti greitai rasti sprendimą, kai visi atrodo sutrikę. Aš jai labai dėkingas.

Iš įvairių viso pasaulio policijos pajėgų atstovų, kurie su manimi aptarinėjo Tamsiąją rinką, turiu paminėti FTB agentą Keithą J. Mularskį, Turkijos kovos su kontrabanda ir organizuotu nusikalstamumu skyriaus inspektorių Bilalą Şeną ir Hambersaido policijos detektyvą seržantą Chrisą Dawsoną. Visi trys paskyrė daug savo brangaus laiko pokalbiams su manimi, kuo puikiausiai mane apšvietė ir visada džiaugėsi galėdami išaiškinti tai, ko aš nebuvau

iki galo perpratęs. Taip pat norėčiau padėkoti pareigūnams iš Sunkių organizuotų nusikaltimų agentūros Londone ir Christianui Aghroumui iš Centrinio biuro kovai su nusikaltimais, susijusiais su informacinėmis ir ryšio technologijomis OCLCTIC Paryžiuje.

Iš kitos pusės, RioRita iš Ukrainos buvo tikras informacijos apie „CarderPlanet", ir ne tik apie ją, lobynas – mano ypatinga padėka jam. Ne mažiau informacijos apie esminius dalykus, susijusius su kibernetiniais nusikaltimais, aš gavau iš Raudonosios Brigados. Esu jam labai dėkingas už draugiškumą ir geranoriškus atsakymus į daugybę mano prašymų pateikti informaciją ir analizę.

Matrica ir JiLsi visada buvo pasirengę pasidalyti žiniomis apie visas Tamsiosios rinkos smulkmenas ir įvertinti tam tikrus įvykius. Pitsburge sužinojau, kad Maksas Vizija yra puikus ir naudingas pašnekovas. Visiems trims mano nuoširdi padėka.

Çağatay'us Evyapanas ir Mertas Ortaças, nors ir nesutaria tarpusavyje, buvo dvi įdomiausios asmenybės, kurias sutikau per pastaruosius trejus metus. Kad ir kokia sudėtinga dabar būtų jų padėtis, norėčiau išreikšti savo dėkingumą jiems abiem.

Estijoje Madis Tuuras išsamiai supažindino mane su šalies politika ir istorija, jau nekalbant apie jo svetingumą ir norą sudominti ir pralinksminti.

Taip pat ačiū CBC korespondentui Brooksui Decilliai iš Kalgario už jo pasiaukojančius tyrimus. Panašiai Stokholme man į pagalbą atėjo Danielis Goldbergas ir Linus Larssonas.

Du žmonės pagelbėjo man techniniais klausimais. Visada galėjau kreiptis į Mikko Hypponeną, kompanijos „F-Secure" Helsinkyje vyriausiąjį tyrimų skyriaus pareigūną, ir Vincentą Diazą iš „Kaspersky Labs" Barselonoje, prašydamas padėti išsiaiškinti dalykus, kurių paprasčiausiai negalėdavau suprasti. Taip pat daug protingų patarimų bendresniais kibernetinio saugumo klausimais gavau iš Rexo Hugheso, dirbančio Wolfsono koledže Kembridže.

Taip pat noriu padėkoti toliau išvardytiems žmonėms, kurie įvairiais būdais man padėjo: Allison Culliford, Luke'ui Dembosky, Sophie Devonshire, Jorisui Eversui, detektyvui Spenceriui Frizzelliui, Tamarai Glenny, Camino Kavanagh, Suatui Kiniklioglu, Dirkui Kolbergui, Darryllui Leaningui, Melissai Llewelyn-Davies, Janei McClellan Q. C., Markui Medishui, Steve'ui Milneriui, Jaanui Prisaalu, Colinui Robinsonui, Anyai Stiglitz ir Eneken Tikk.

Man labai daug padėjo mano agentai ir leidėjai. Clare Conville iš Londono yra tokia puiki agentė, kokią tik įmanoma įsivaizduoti, o jai talkina nuostabi komanda. Michaelis Carlisle taip pat energingai padeda Niujorke. Man pasisekė, nes turėjau tris redaktorius: Willį Sulkiną iš „The Bodley Head", Daną Franką iš „Knopf" ir Sarah MacLachlan iš „Anansi Press", kurių dėka rašymo patirtis tapo lengviau įvaldoma, o galutinio produkto vertė smarkiai padidėjo. Jei įsivėlė kokių klaidų, aš, savaime suprantama, prisiimu už jas visišką atsakomybę. Taip pat norėčiau padėkoti dar dviem žmonėms, turėjusiems didelę įtaką knygai: Kay Peddle iš „The Bodley Head" ir Janie Yoon iš „Anasi".

Trys mano vaikai, kuriems dedikuotas šis darbas, neprarado sveiko susidomėjimo šia knyga, nors kol rašiau, manęs dažnai nebūdavo arba būdavau išsiblaškęs. Jie visada buvo mieli ir palaikė mane.

Ir galiausiai padėką ir meilę skiriu savo žmonai Kirsty Lang, kuri komentavo, kritikavo, pataikavo ir visą laiką palaikė mano dvasią. Ne pirmą kartą be jos aš nebūčiau to padaręs.

2011 m. birželis

Misha Glenny
Nematoma rinka
Elektroniniai nusikaltimai ir jūs

Vertėja
Marija Dalia Tručinskienė

Redaktorė
Dalia Kižlienė

Dailininkas
Zigmantas Butautis

Maketavo
Audris Šimakauskas

Tiražas 2 000 egz.
Išleido UAB „Baltų lankų“ leidyba
Palangos g. 4, LT-01402 Vilnius
leidykla@baltoslankos.lt
www.baltoslankos.lt

Spausdino spaustuvė AB „Spauda“
Laisvės pr. 60, LT-05120 Vilnius
www.spauda.com

Gyvenimas skaitmenizuotoje globalioje visuomenėje turi daug pranašumų. Tačiau kelia ir daug pavojų. Mes tampame vis labiau priklausomi nuo skaitmeninio pasaulio: naudojamės internetine bankininkyste, apsiperkame internetu, virtualiai bendraujame su draugais, dirbame ir leidžiame laisvalaikį. Bet ar tos institucijos, kurios mus saugo gatvėse, jau išmoko mus apsaugoti ir virtualioje erdvėje? O gal mes per daug pasikliaujame saugumo iliuzija ir pernelyg lengva ranka dalijamės savo asmeniniu gyvenimu ir mintimis su tais, kurie gali lengvai tuo pasinaudoti?

Šioje knygoje atskleidžiamos trys pagrindinės grėsmės, su kuriomis šiandien susiduriame: skaitmeniniai nusikaltimai, skaitmeniniai karai ir skaitmeninis pramoninis šnipinėjimas. Kiekvienais metais vyriausybės ir privatus sektorius praranda milžiniškas pinigų sumas, kovodami su dažnai nematomu ir itin gudriu naujo pobūdžio nusikaltėliu – programišiumi.

Tyrinėdamas realius virtualiame pasaulyje vykdomus nusikaltimus ir įvairių šalių pareigūnų kovą su jais, Misha Glenny išmaišė visą pasaulį ir atvirai kalbėjosi su kibernetiniais nusikaltėliais, kompiuterių fanatikais, kompiuterinio saugumo ekspertais, policijos atstovais ir nusikaltimų aukomis. Jo tyrinėjimų rezultatas – mūsų dienomis itin aktuali knyga, privaloma kiekvienam, besinaudojančiam kompiuteriu.

Ši itin paveiki knyga atskleidžia, kaip beviltiškai mums trūksta bendrų tarptautinių įrankių kovoti su skaitmeniniu nusikalstamumu. Būtina perskaityti.

Roberto Saviano,
knygos *Gomora* autorius

ISBN 978-9955-23-620-7

www.baltoslankos.lt